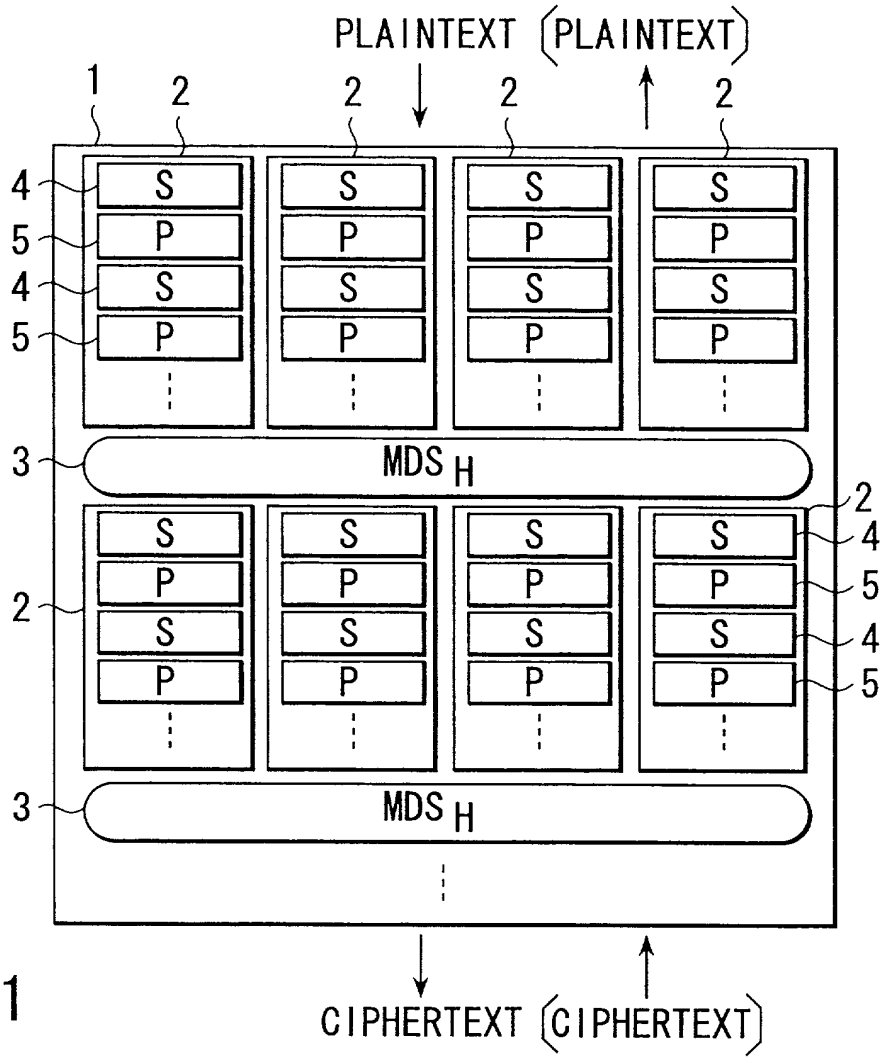

PLAINTEXT (PLAINTEXT)
1
2
2
2
2
4
5
4
5
S
P
3
MDS H
2
CIPHERTEXT (CIPHERTEXT)

FIG. 1

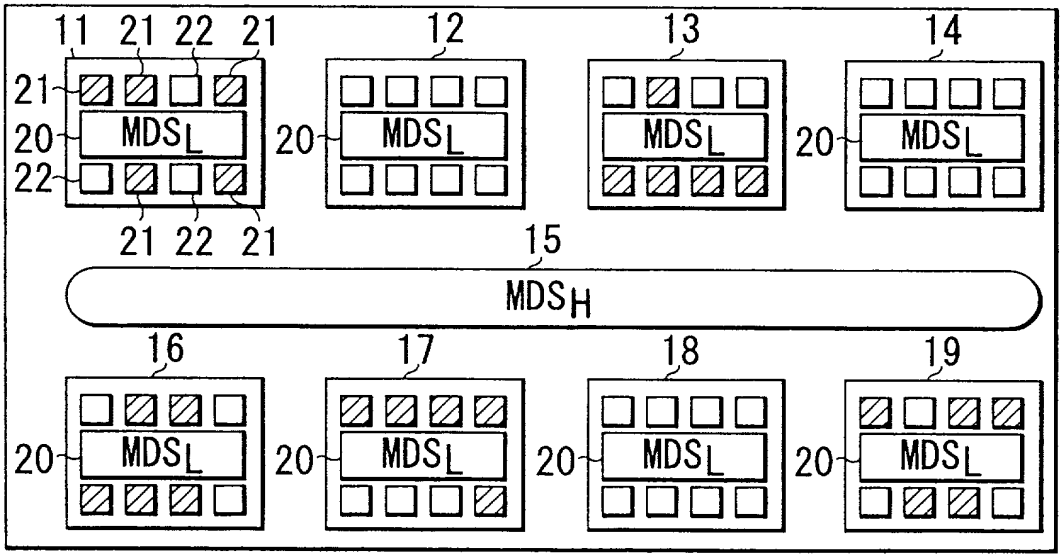

11
21
22
21
12
13
14
20
MDSL
22
15
MDSH
16
17
18
19

FIG. 2

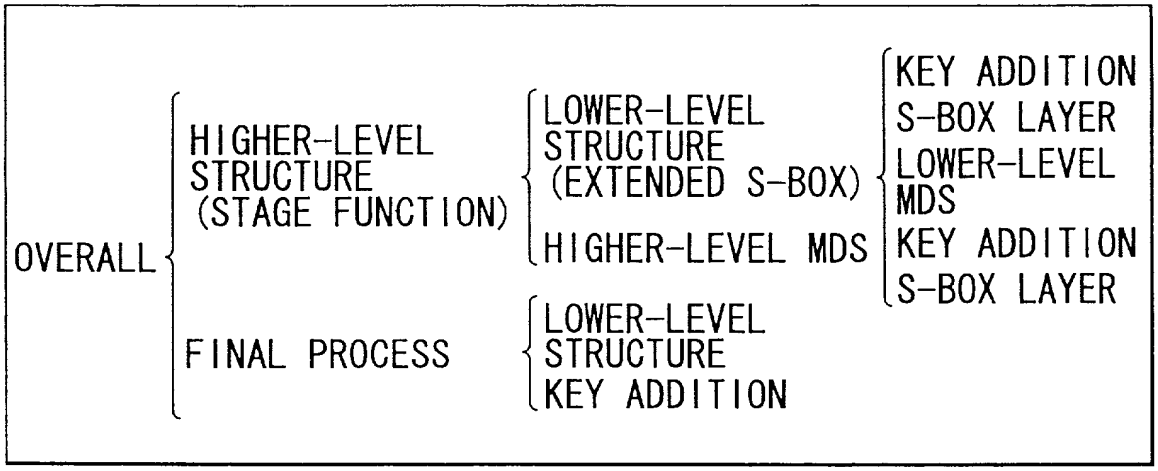

OVERALL
HIGHER-LEVEL STRUCTURE (STAGE FUNCTION)
LOWER-LEVEL STRUCTURE (EXTENDED S-BOX)
KEY ADDITION
S-BOX LAYER
LOWER-LEVEL MDS
HIGHER-LEVEL MDS
KEY ADDITION
S-BOX LAYER
FINAL PROCESS
LOWER-LEVEL STRUCTURE
KEY ADDITION

FIG. 3

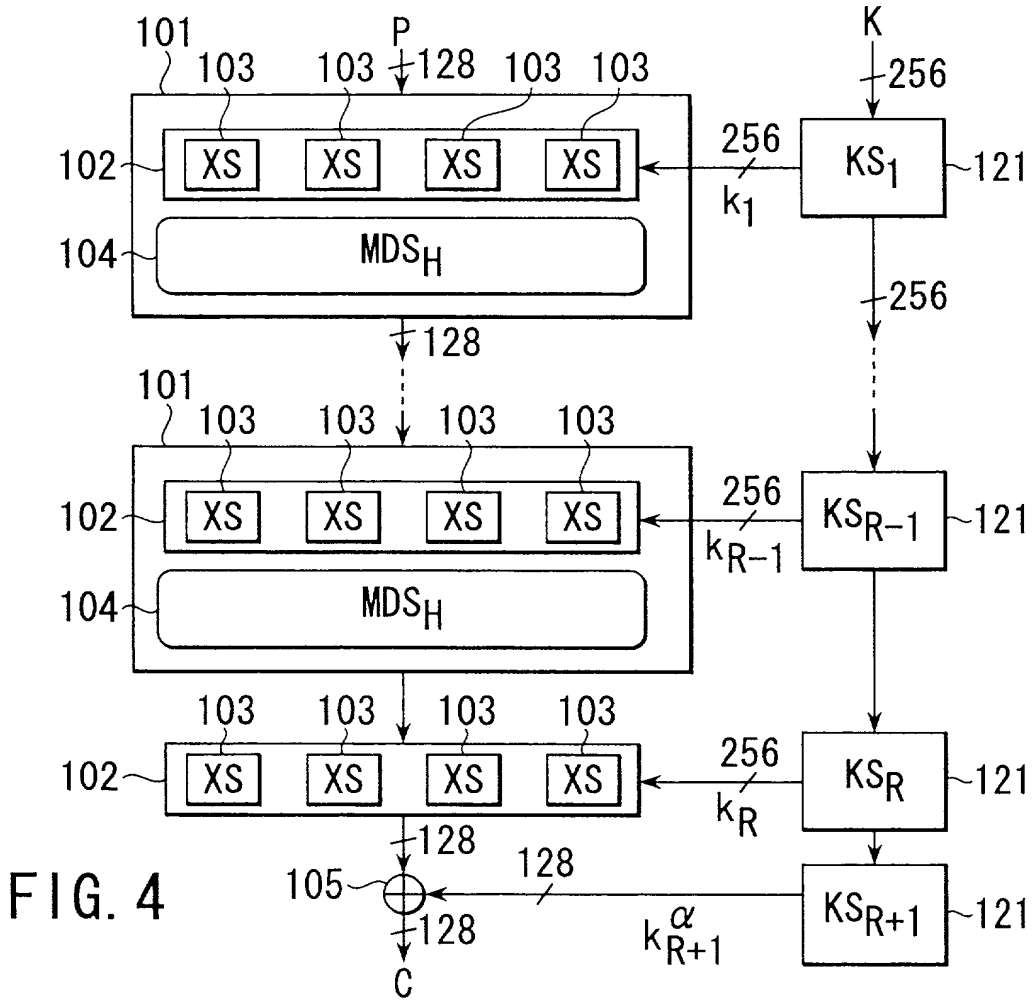

101
P
K
103
128
256
102
XS
104
MDS_H
KS_1
KS_R-1
KS_R
KS_R+1
121
k_1
k_R-1
k_R
105
C

FIG. 4

```
s[256]={
   72 AA 49 16 1E 3A 43 AE 66 BC 00 73 79 3B FB 9F
   69 6A A2 50 6E F5 EF AC 22 02 AD 26 E2 DF 97 F0
   9E BF 17 8B FA 7C F4 71 7F CA F6 52 FD C3 E5 64
   53 8D E0 F3 0F 78 CB 9B 68 3C 0D 1F 89 B6 EB F7
   44 4A 06 A6 56 6B 85 01 30 88 51 31 9C A0 A3 25
   60 5B FF 05 B7 91 15 B3 A9 20 03 2B 61 42 95 4D
   F9 7E 0E E9 D8 F1 46 99 CE BE D9 54 80 B0 D2 4F
   7A E8 35 92 1B 7B 12 D6 4C D5 E7 EE B1 24 DE 21
   04 10 AB 29 9A 81 FE A7 B8 63 28 0A 8A D1 C6 07
   B9 C8 98 82 74 9D 84 47 94 C7 6C 11 D7 BA C1 C9
   DD 77 39 2F 2E C2 67 41 E4 58 34 CD 1C 93 96 7D
   2C F8 B5 70 14 08 DC CC 87 D0 5E 32 C5 C4 59 3E
   CF 55 5C 23 75 2D 2A 86 4B 1D 5F E6 FC B2 4E 09
   27 AF 19 B4 BD 6D 3D 6F ED 62 EA F2 D3 36 38 DB
   BB 83 45 37 A4 EC 8C 5D E1 33 90 A1 40 8E 1A A5
   0B 3F 5A DA 13 76 0C C0 48 E3 65 A8 18 8F D4 57 }
```

112

FIG. 5

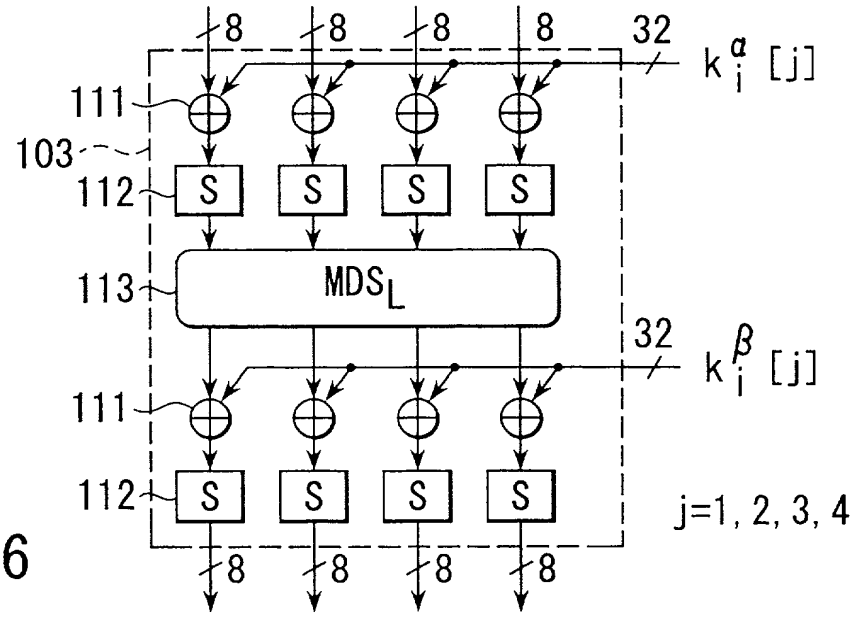


FIG. 6

FIG. 7

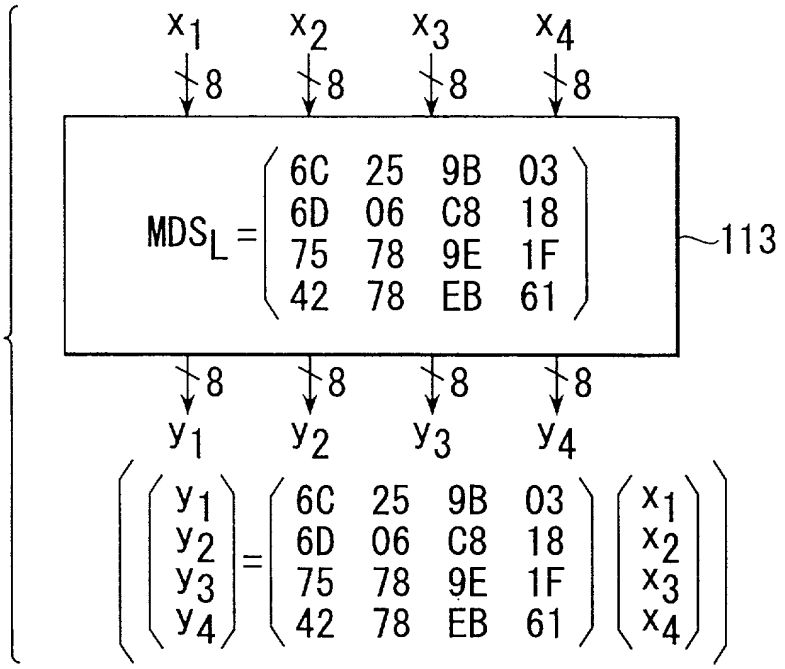


FIG. 8

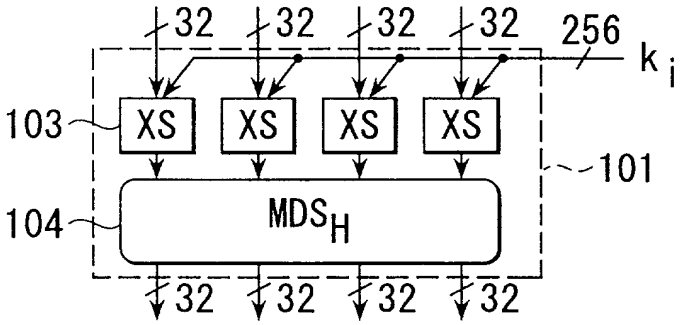
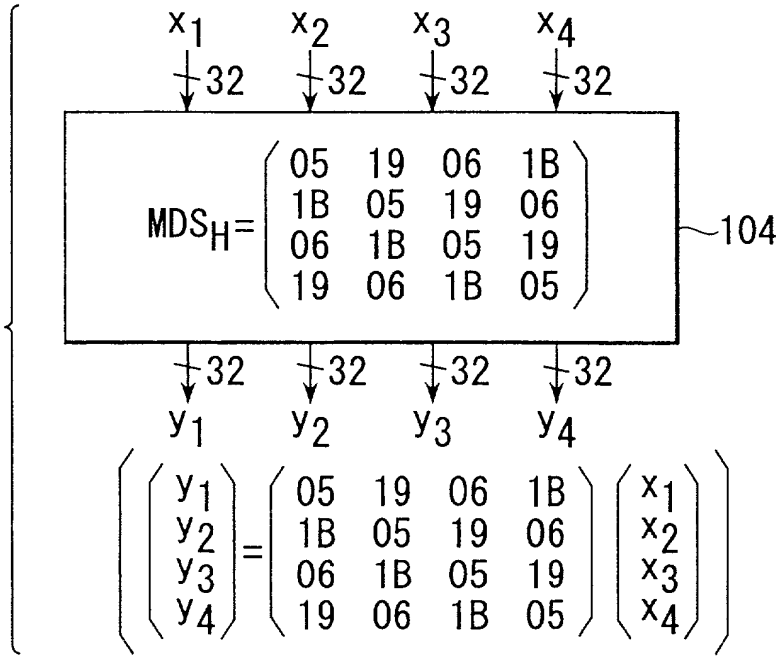
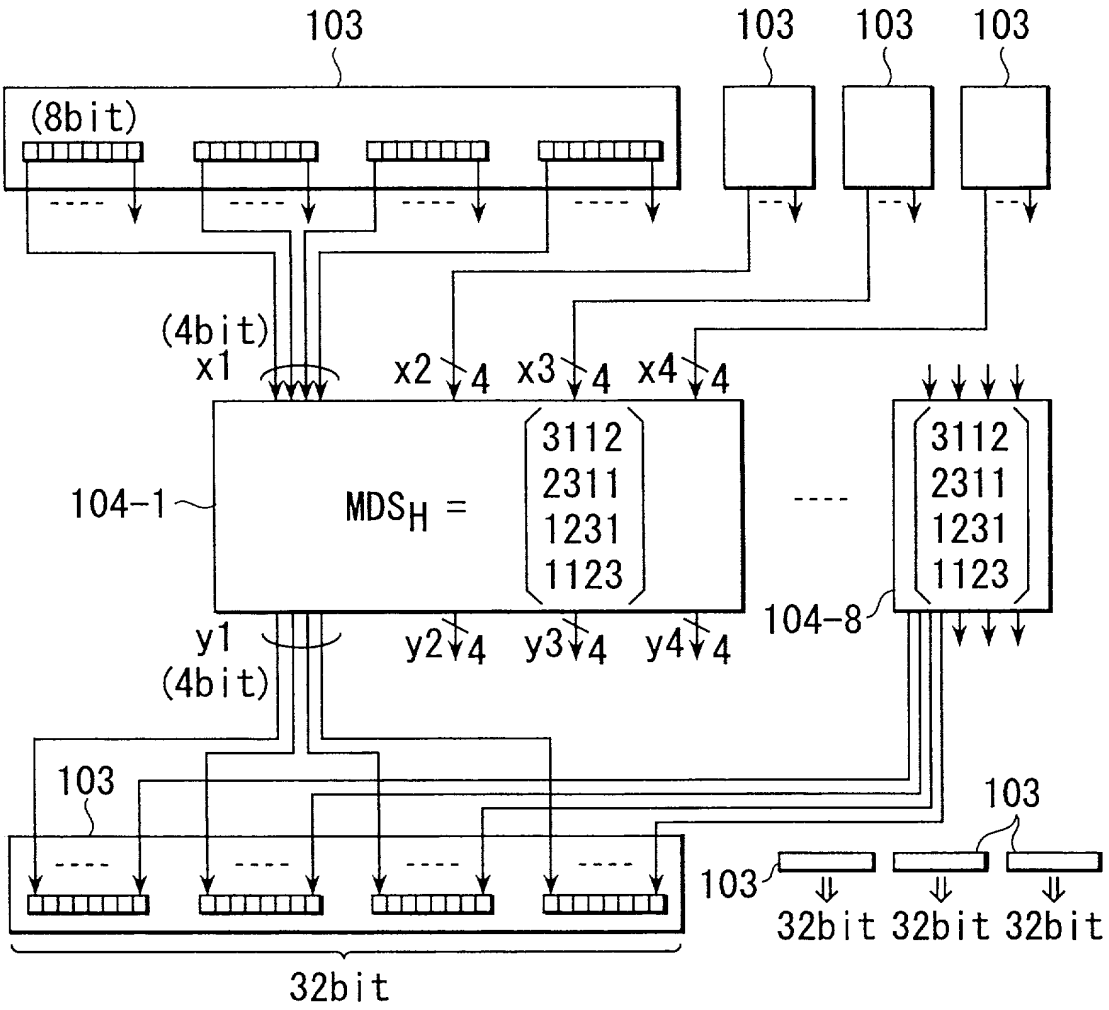


FIG. 9





$$\begin{pmatrix} y1 \\ y2 \\ y3 \\ y4 \end{pmatrix} = \begin{pmatrix} 3112 \\ 2311 \\ 1231 \\ 1123 \end{pmatrix} \begin{pmatrix} x1 \\ x2 \\ x3 \\ x4 \end{pmatrix}$$

FIG. 10

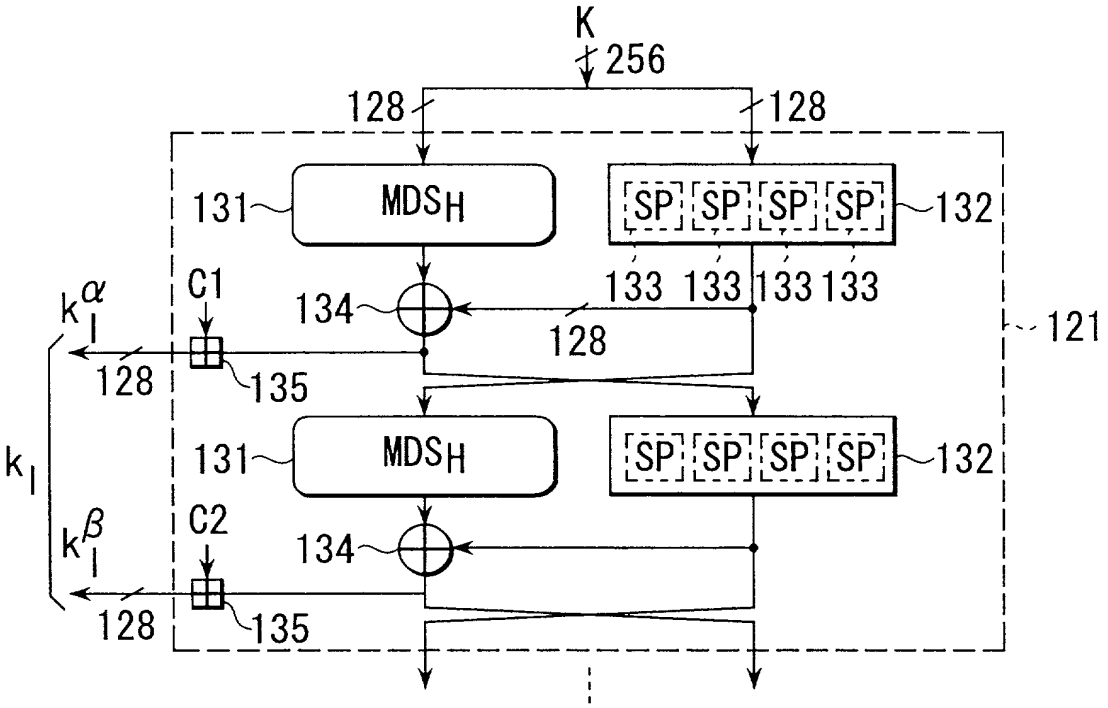

K
256
128
128
131
MDSH
SP SP SP SP
132
133 133 133 133
C1
134
128
121
k_l^{α}
128
135
131
MDSH
SP SP SP SP
132
k_l
C2
134
k_l^{β}
128
135

FIG. 11

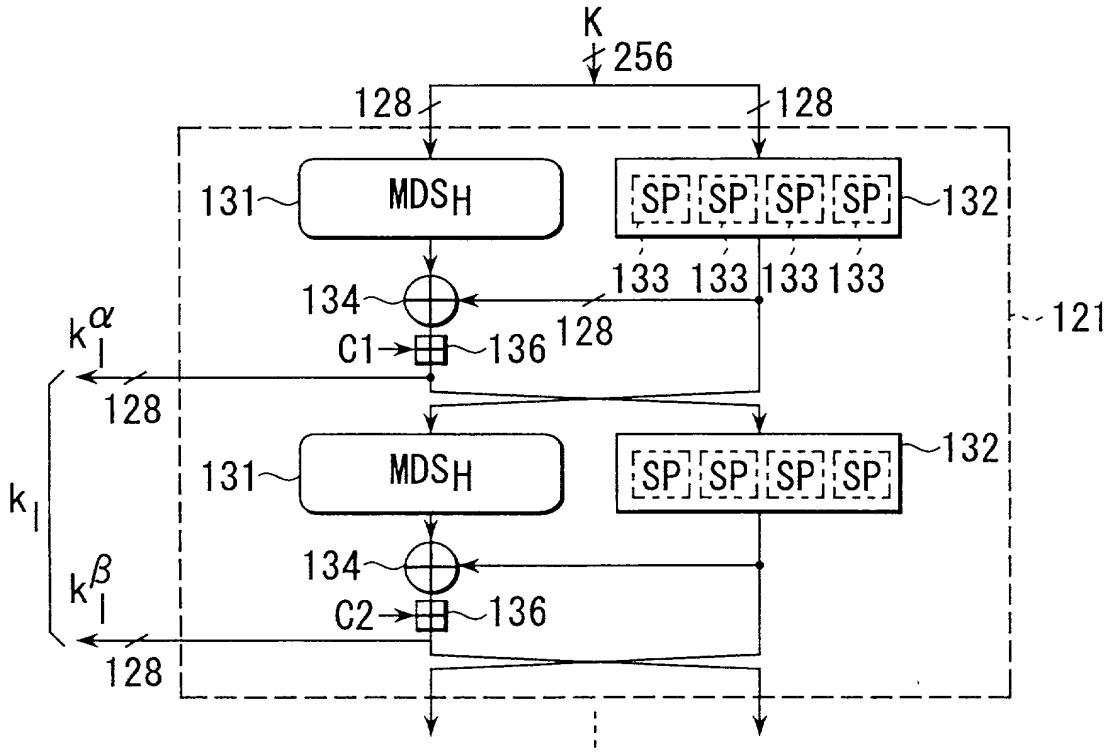

K
256
128
128
131
MDSH
SP SP SP SP
132
133 133 133 133
134
128
121
C1
136
k_l^{α}
128
131
MDSH
SP SP SP SP
132
k_l
134
C2
136
k_l^{β}
128

FIG. 12

FIG. 13

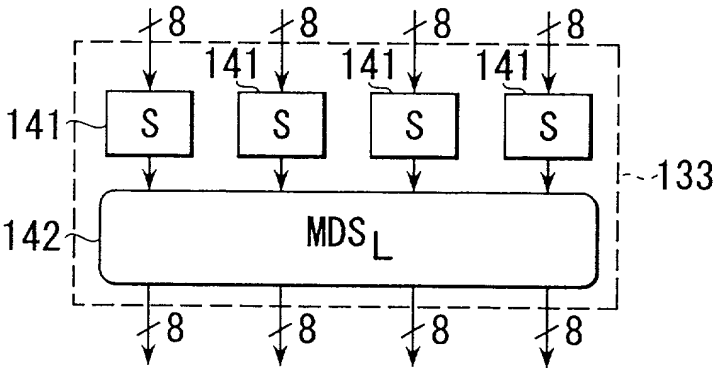


FIG. 14

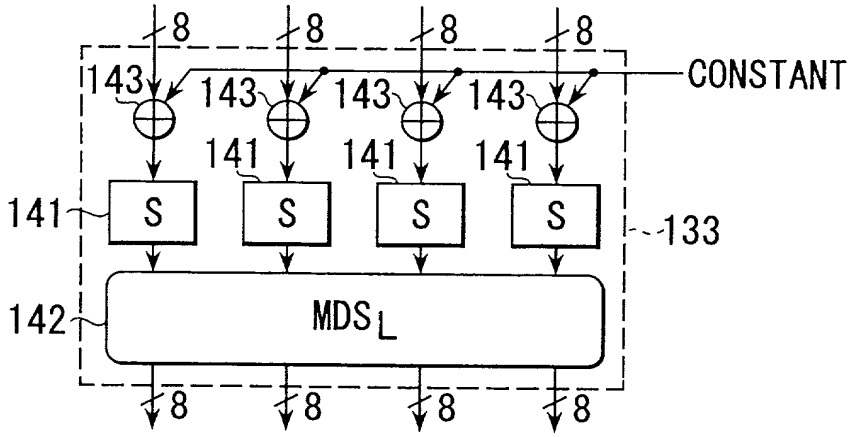


FIG. 15

C1	(H2, H0, H1, H1)
C2	(H3, H2, H0, H3)
C3	(H1, H0, H0, H0)
C4	(H1, H0, H1, H3)
C5	(H0, H1, H0, H2)
C6	(H3, H2, H0, H0)
C7	(H1, H2, H1, H0)
C8	(H2, H1, H2, H3)
C9	(H2, H1, H0, H0)
C10	(H1, H1, H1, H2)
C11	(H3, H1, H1, H2)
C12	(H1, H1, H2, H0)
C13	(H1, H3, H3, H1)
C14	(H2, H3, H3, H1)
C15	(H1, H3, H1, H0)
C16	(H1, H0, H0, H3)
C17	(H1, H2, H0, H3)

WHERE

$H0 = (5A827999)_H = \lfloor \sqrt{2}/4 \times 2^{32} \rfloor$

$H1 = (6ED9EBA1)_H = \lfloor \sqrt{3}/4 \times 2^{32} \rfloor$

$H2 = (8F1BBCDC)_H = \lfloor \sqrt{5}/4 \times 2^{32} \rfloor$

$H3 = (CA62C1D6)_H = \lfloor \sqrt{10}/4 \times 2^{32} \rfloor$

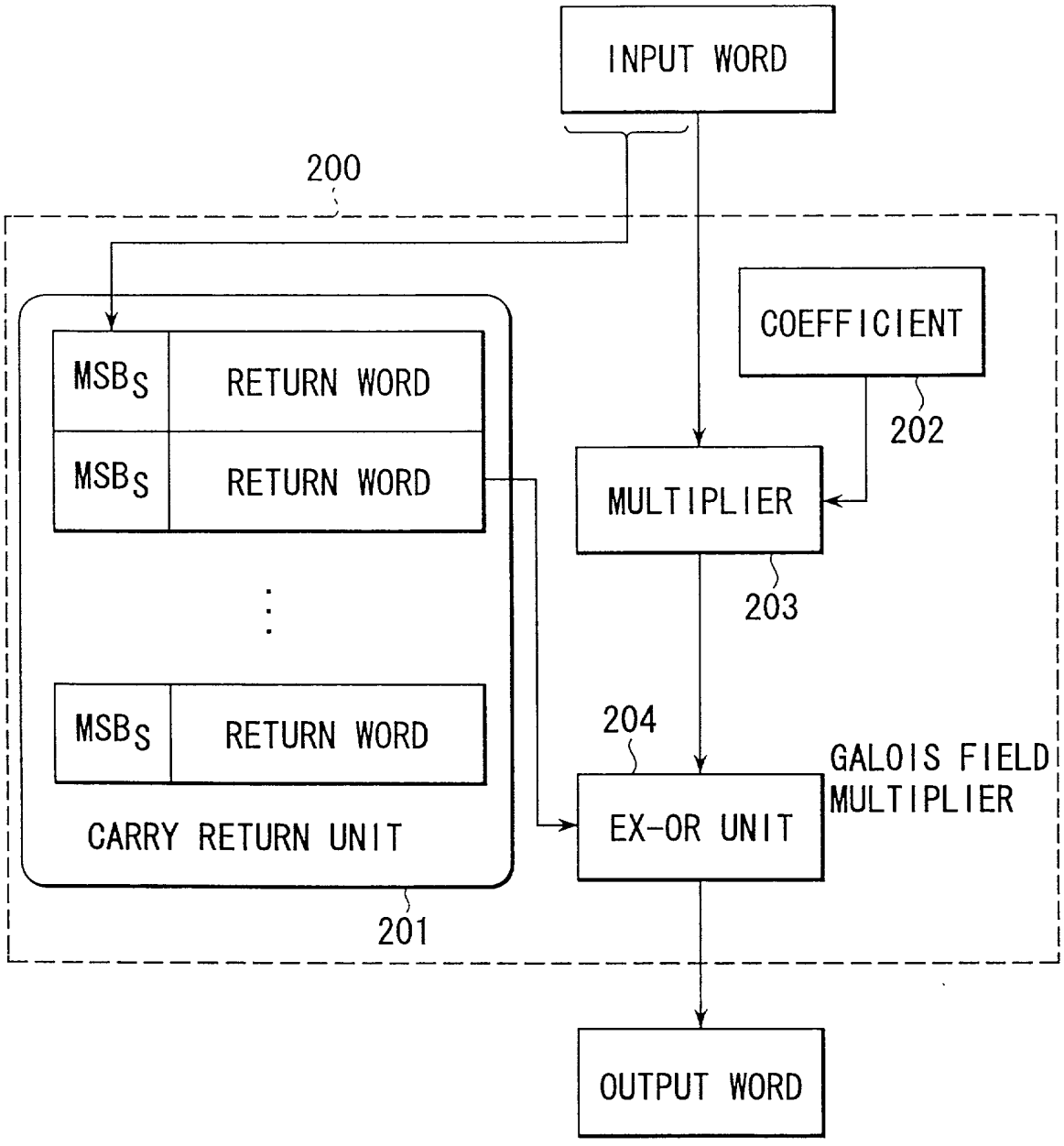

INPUT WORD
200
COEFFICIENT
202
MSBs
RETURN WORD
MSBs
RETURN WORD
MULTIPLIER
203
MSBs
RETURN WORD
204
GALOIS FIELD MULTIPLIER
EX-OR UNIT
CARRY RETURN UNIT
201
OUTPUT WORD

FIG. 16

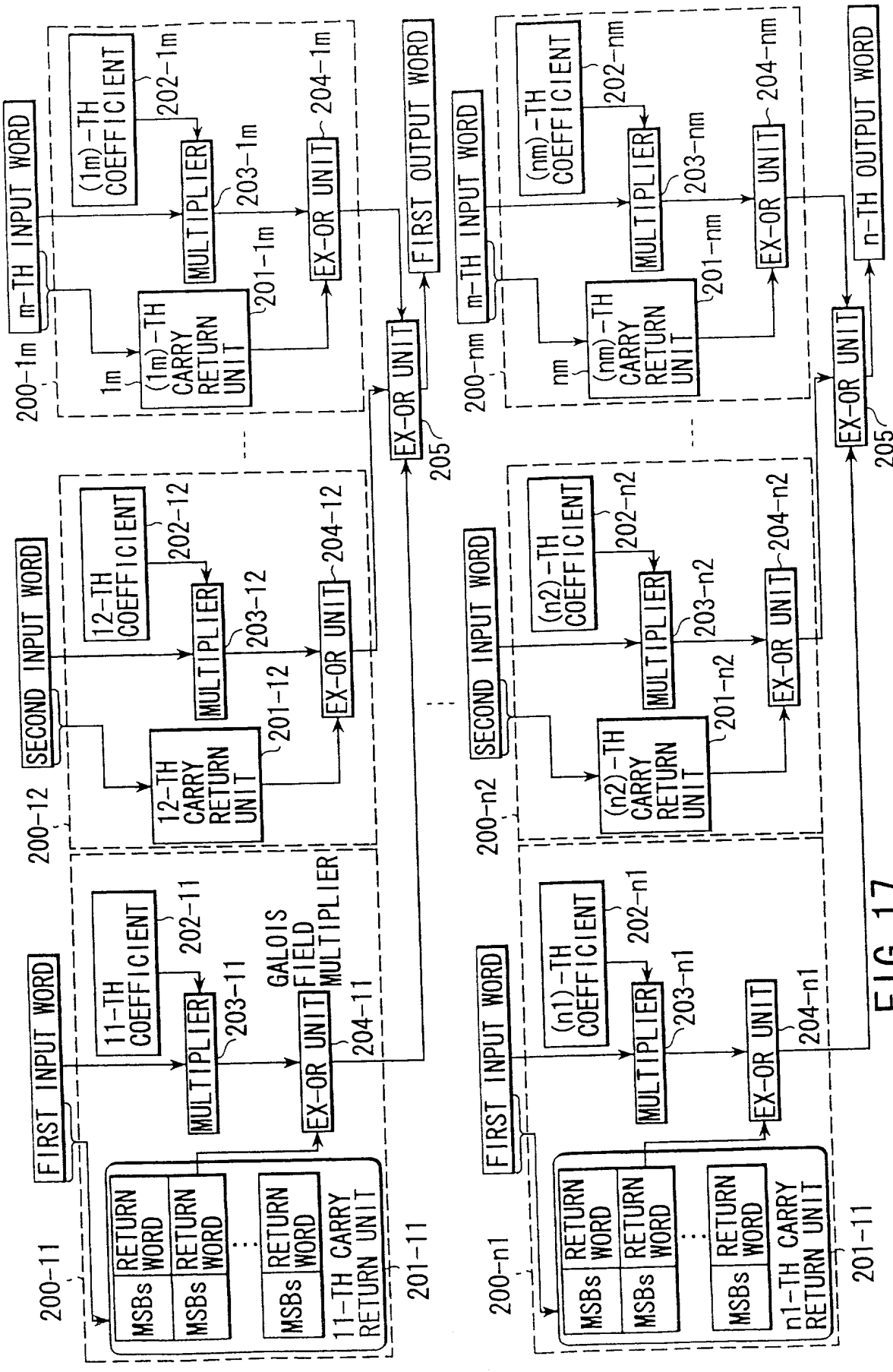

200-11
FIRST INPUT WORD
11-TH COEFFICIENT
202-11
MULTIPLIER
203-11
GALOIS FIELD MULTIPLIER
EX-OR UNIT
204-11
MSBs
RETURN WORD
11-TH CARRY RETURN UNIT
201-11
200-12
SECOND INPUT WORD
12-TH COEFFICIENT
202-12
MULTIPLIER
203-12
EX-OR UNIT
204-12
12-TH CARRY RETURN UNIT
201-12
200-1m
m-TH INPUT WORD
(1m)-TH COEFFICIENT
202-1m
MULTIPLIER
203-1m
EX-OR UNIT
204-1m
1m
(1m)-TH CARRY RETURN UNIT
201-1m
EX-OR UNIT
205
FIRST OUTPUT WORD
200-n1
FIRST INPUT WORD
(n1)-TH COEFFICIENT
202-n1
MULTIPLIER
203-n1
EX-OR UNIT
204-n1
n1-TH CARRY RETURN UNIT
200-n2
SECOND INPUT WORD
(n2)-TH COEFFICIENT
202-n2
MULTIPLIER
203-n2
EX-OR UNIT
204-n2
(n2)-TH CARRY RETURN UNIT
201-n2
200-nm
m-TH INPUT WORD
(nm)-TH COEFFICIENT
202-nm
MULTIPLIER
203-nm
EX-OR UNIT
204-nm
nm
(nm)-TH CARRY RETURN UNIT
201-nm
EX-OR UNIT
205
n-TH OUTPUT WORD

FIG. 17

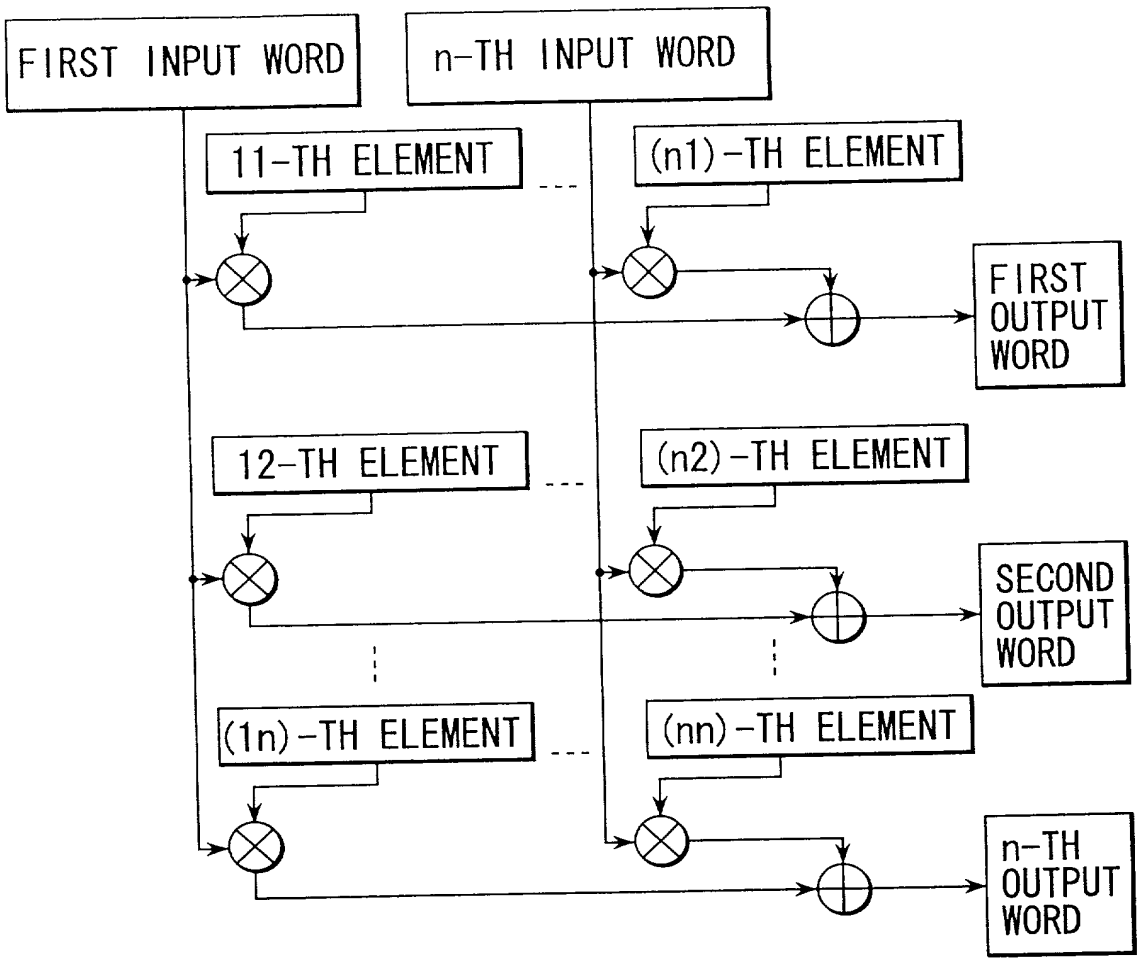

FIRST INPUT WORD
n-TH INPUT WORD
11-TH ELEMENT
(n1)-TH ELEMENT
FIRST OUTPUT WORD
12-TH ELEMENT
(n2)-TH ELEMENT
SECOND OUTPUT WORD
(1n)-TH ELEMENT
(nn)-TH ELEMENT
n-TH OUTPUT WORD

FIG. 18

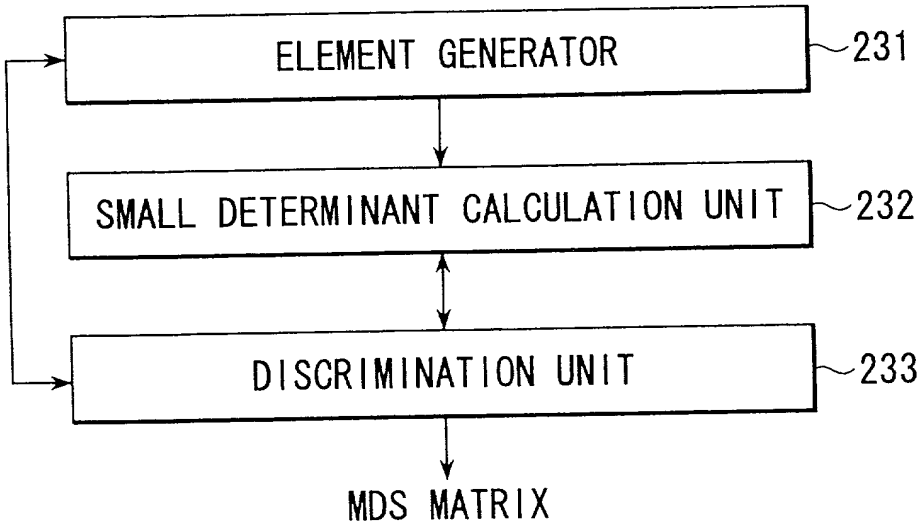

ELEMENT GENERATOR
231
SMALL DETERMINANT CALCULATION UNIT
232
DISCRIMINATION UNIT
233
MDS MATRIX

FIG. 19

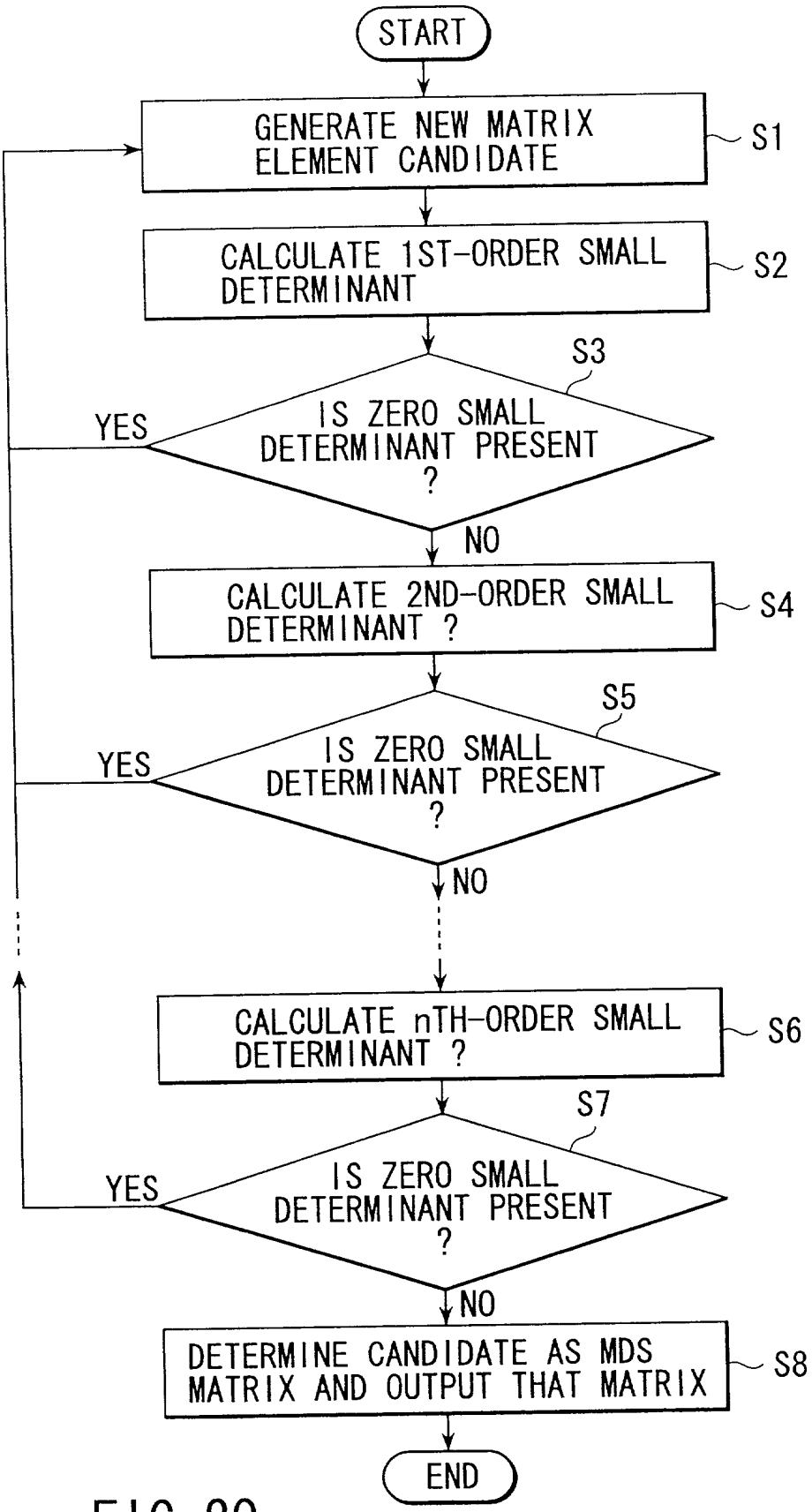

START
GENERATE NEW MATRIX ELEMENT CANDIDATE
S1
CALCULATE 1ST-ORDER SMALL DETERMINANT
S2
S3
IS ZERO SMALL DETERMINANT PRESENT ?
YES
NO
CALCULATE 2ND-ORDER SMALL DETERMINANT ?
S4
S5
IS ZERO SMALL DETERMINANT PRESENT ?
YES
NO
CALCULATE nTH-ORDER SMALL DETERMINANT ?
S6
S7
IS ZERO SMALL DETERMINANT PRESENT ?
YES
NO
DETERMINE CANDIDATE AS MDS MATRIX AND OUTPUT THAT MATRIX
S8
END

FIG. 20

FIG. 21

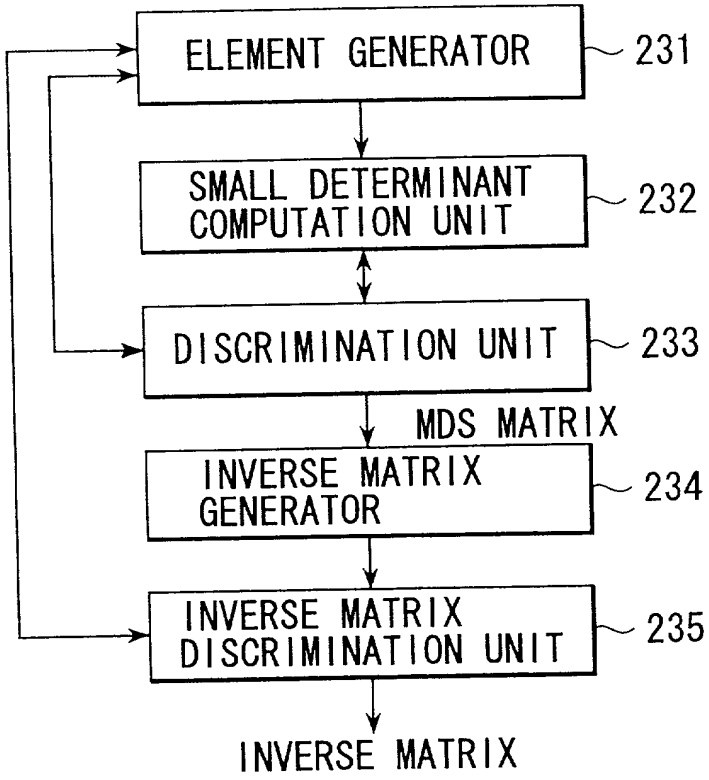
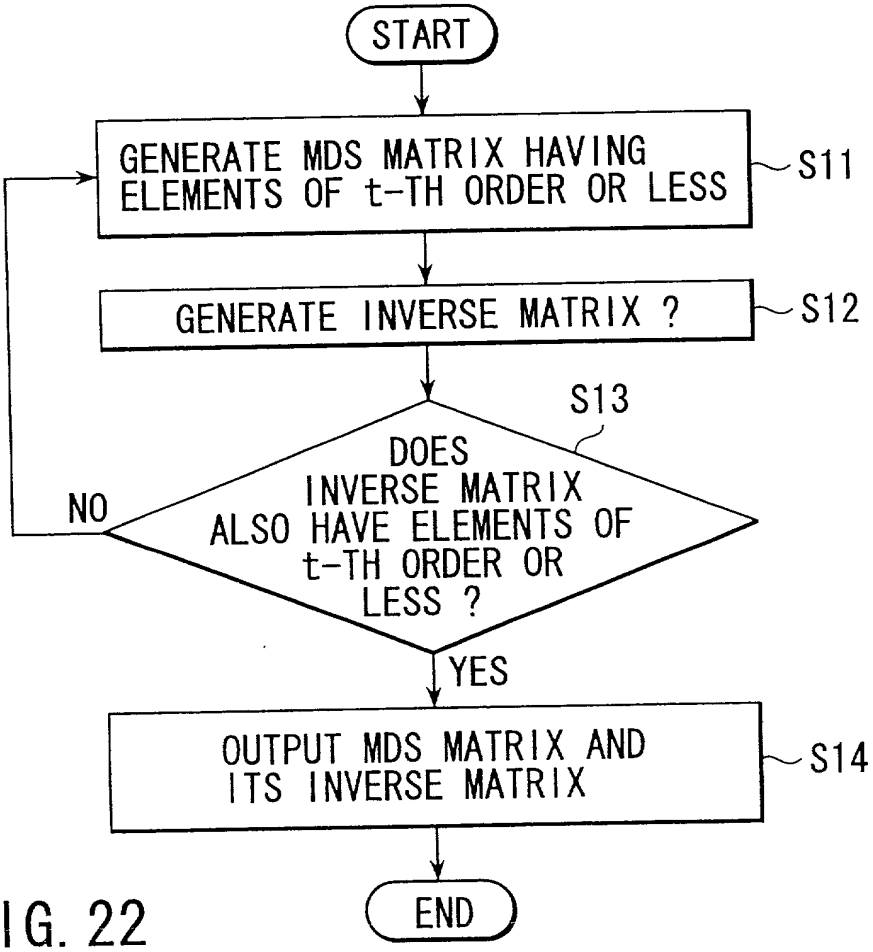

ELEMENT GENERATOR
231
SMALL DETERMINANT COMPUTATION UNIT
232
DISCRIMINATION UNIT
233
MDS MATRIX
INVERSE MATRIX GENERATOR
234
INVERSE MATRIX DISCRIMINATION UNIT
235
INVERSE MATRIX

FIG. 22


START
GENERATE MDS MATRIX HAVING ELEMENTS OF t-TH ORDER OR LESS
S11
GENERATE INVERSE MATRIX ?
S12
S13
DOES INVERSE MATRIX ALSO HAVE ELEMENTS OF t-TH ORDER OR LESS ?
NO
YES
OUTPUT MDS MATRIX AND ITS INVERSE MATRIX
S14
END

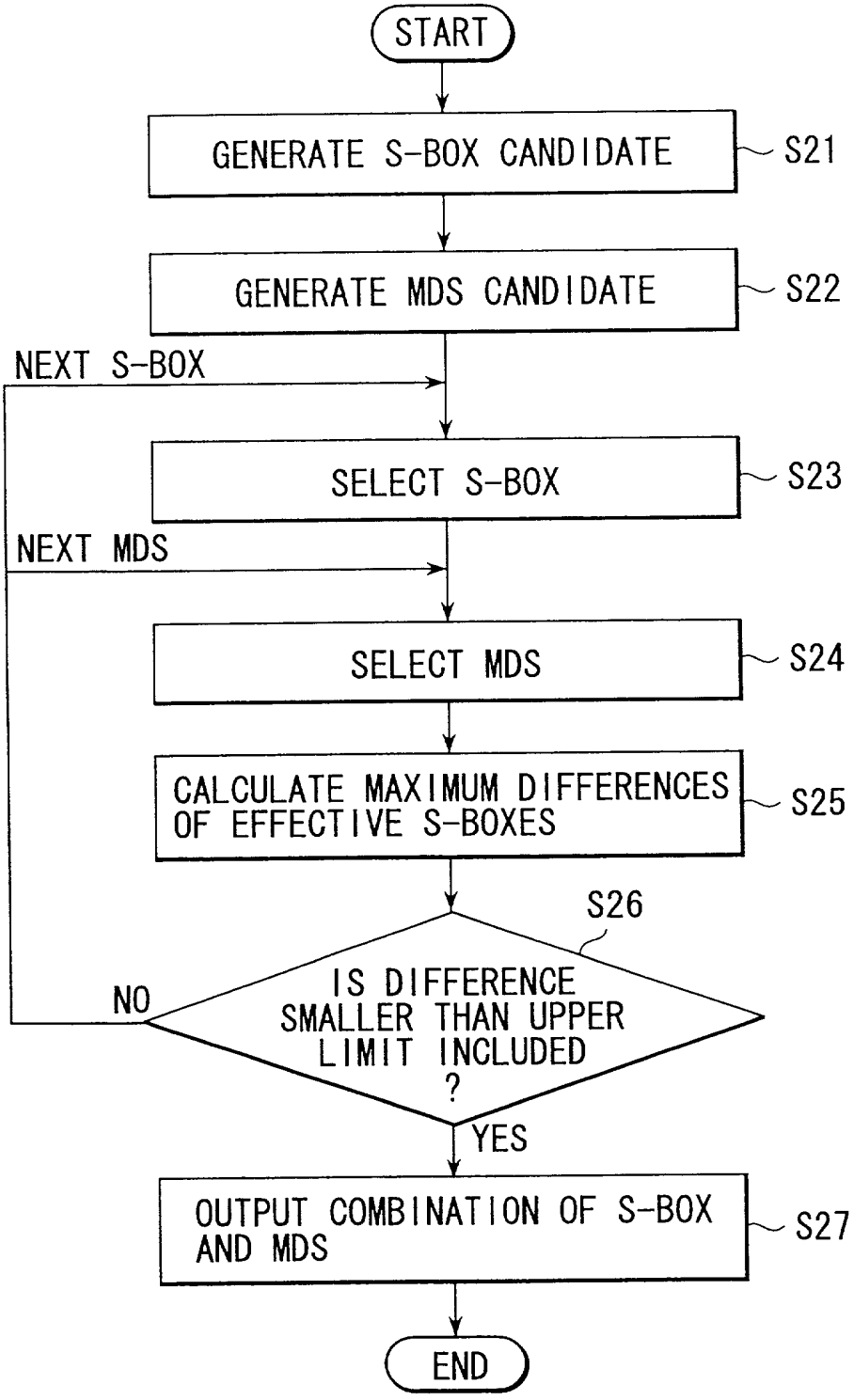

START
GENERATE S-BOX CANDIDATE
S21
GENERATE MDS CANDIDATE
S22
NEXT S-BOX
SELECT S-BOX
S23
NEXT MDS
SELECT MDS
S24
CALCULATE MAXIMUM DIFFERENCES OF EFFECTIVE S-BOXES
S25
S26
IS DIFFERENCE SMALLER THAN UPPER LIMIT INCLUDED ?
NO
YES
OUTPUT COMBINATION OF S-BOX AND MDS
S27
END

FIG. 23

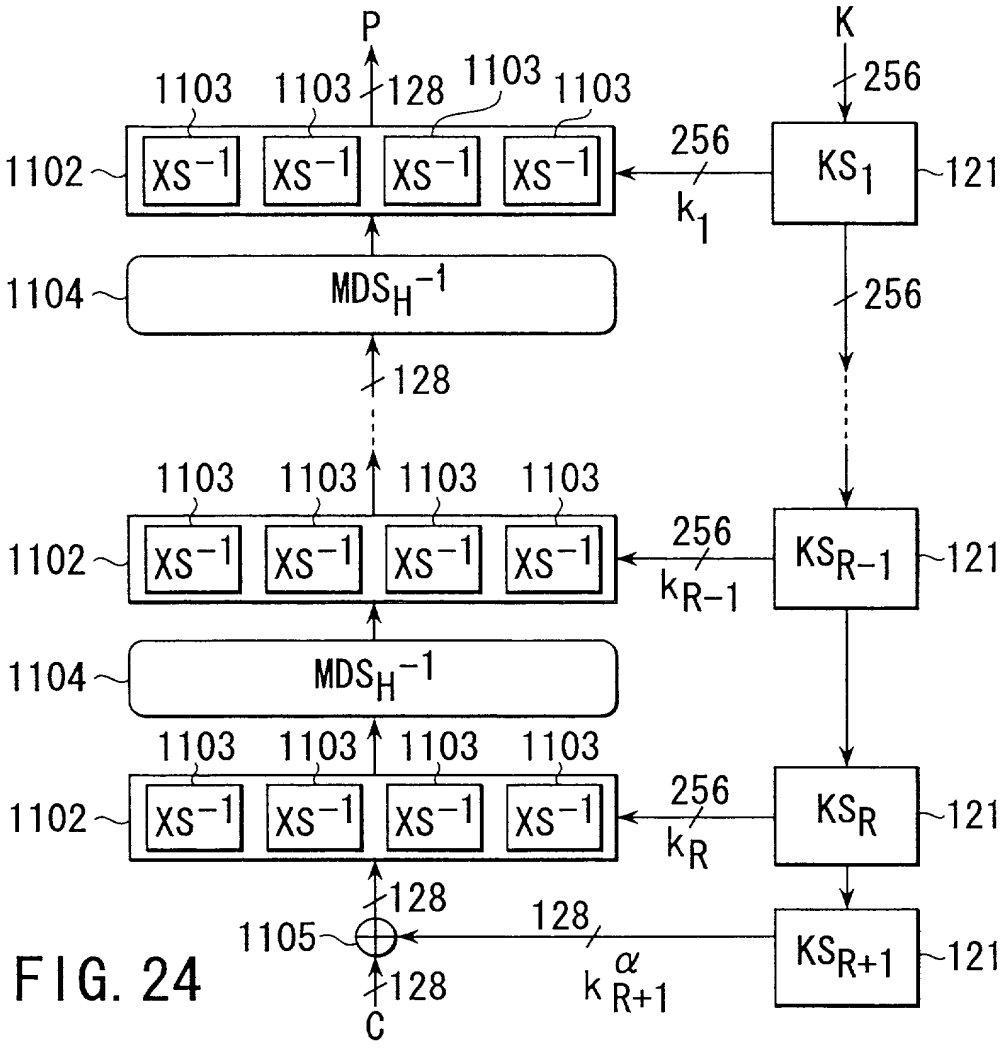

P
K
256
1103
1103
128
1103
1103
1102
XS-1
XS-1
XS-1
XS-1
256
KS1
121
k1
1104
MDSH-1
256
128
1103
1103
1103
1103
1102
XS-1
XS-1
XS-1
XS-1
256
KSR-1
121
kR-1
1104
MDSH-1
1103
1103
1103
1103
1102
XS-1
XS-1
XS-1
XS-1
256
KSR
121
kR
128
1105
128
KSR+1
121
128
k α R+1
C

FIG. 24

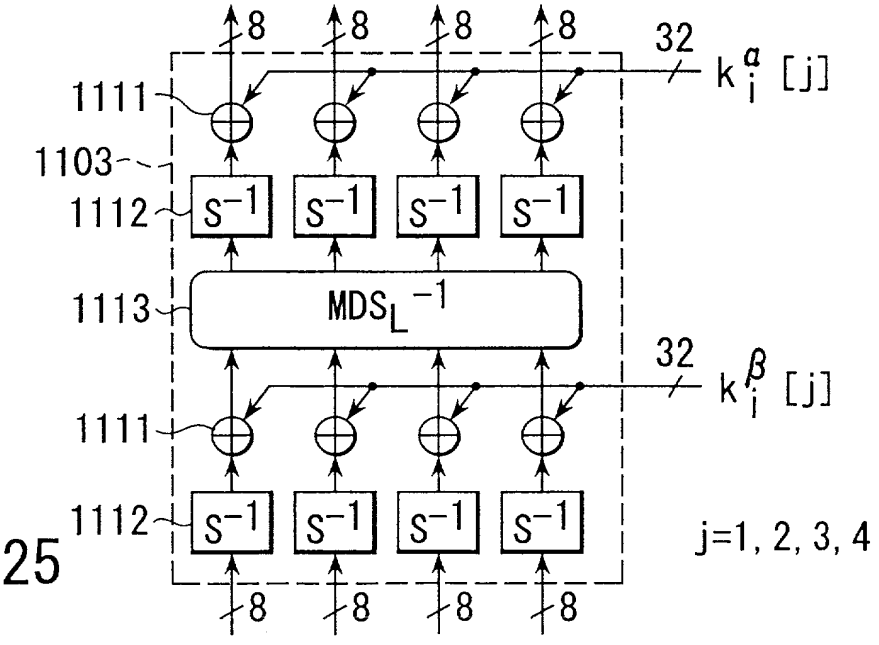

8
8
8
8
32
k a i [j]
1111
1103
1112
S-1
S-1
S-1
S-1
1113
MDSL-1
32
k β i [j]
1111
1112
S-1
S-1
S-1
S-1
8
8
8
8
j=1, 2, 3, 4

FIG. 25

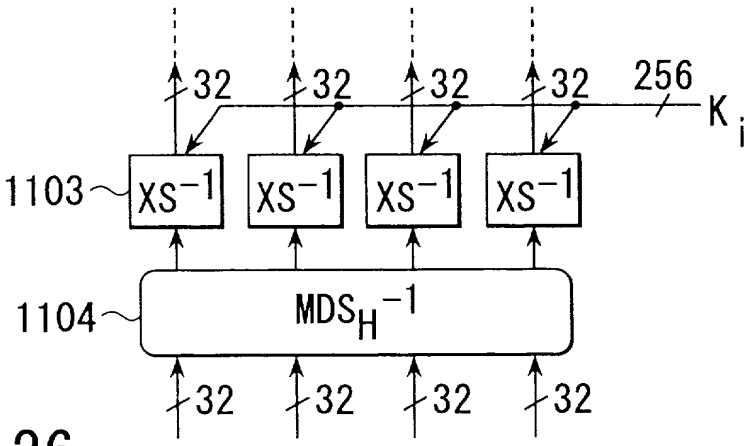

32
32
32
32
256
K_i
1103
XS^{-1}
XS^{-1}
XS^{-1}
XS^{-1}
1104
MDS_H^{-1}
32
32
32
32

FIG. 26

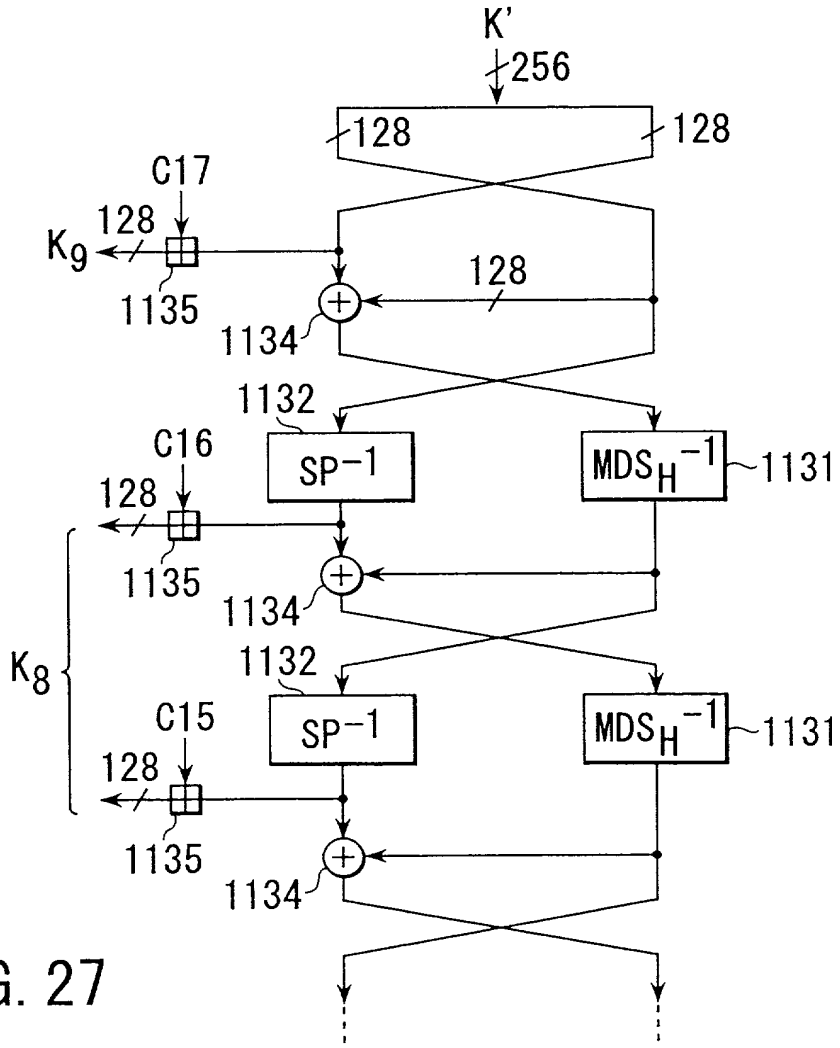

K'
256
128
128
C17
128
K_9
1135
128
1134
1132
C16
SP^{-1}
MDS_H^{-1}
1131
128
1135
1134
K_8
1132
C15
SP^{-1}
MDS_H^{-1}
1131
128
1135
1134

FIG. 27

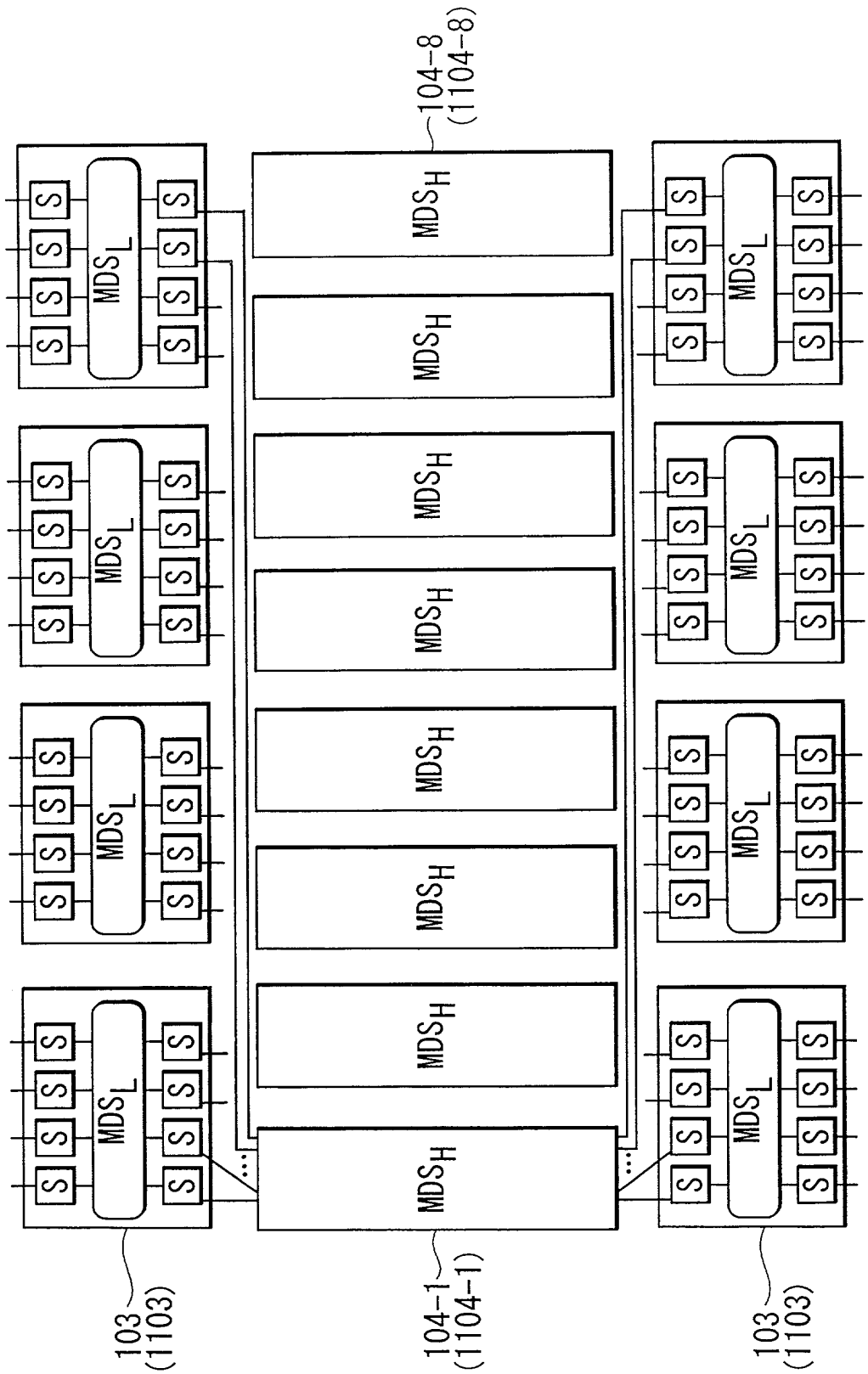


FIG. 28

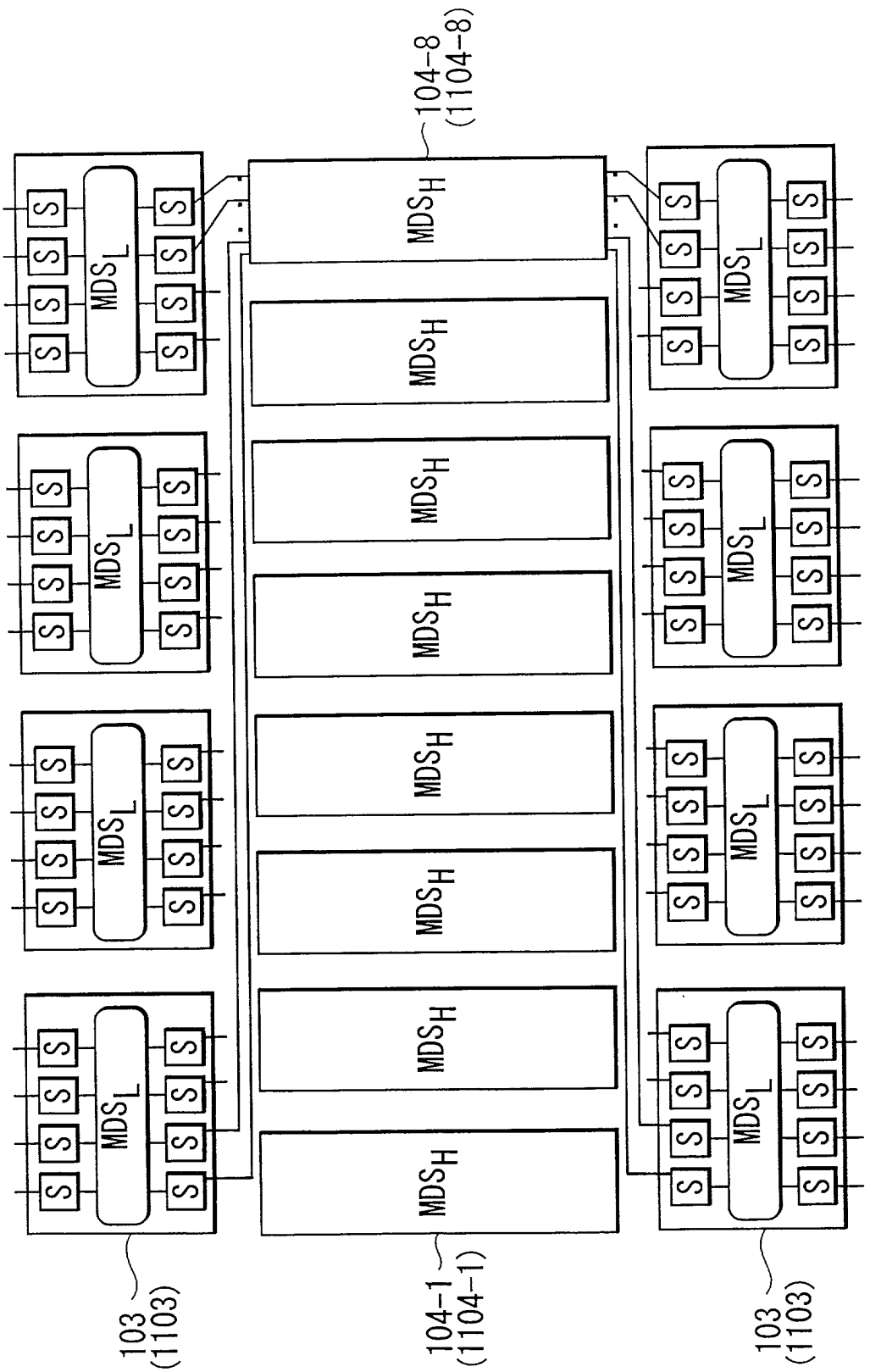


FIG. 29

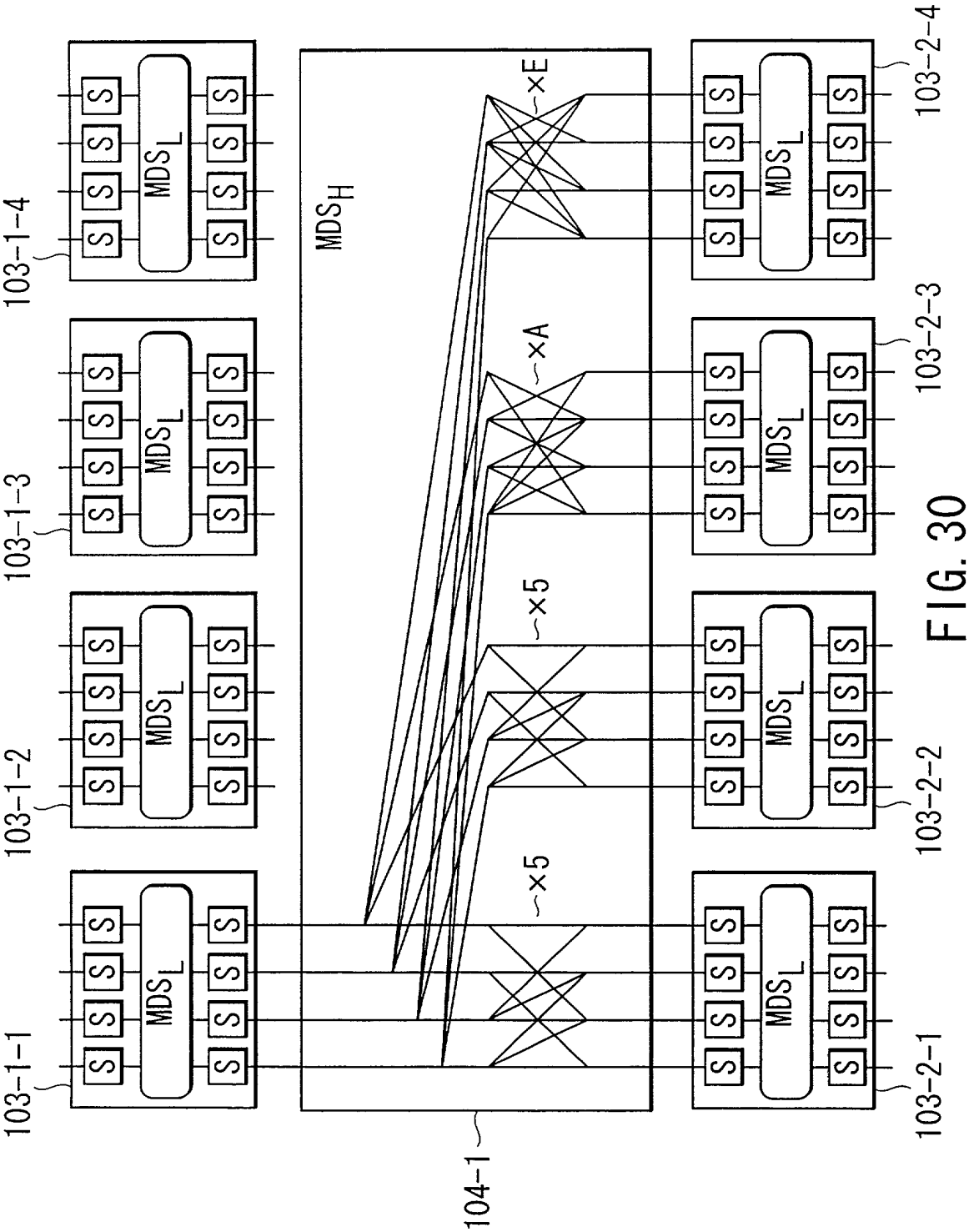

103-1-1
103-1-2
103-1-3
103-1-4
103-2-1
103-2-2
103-2-3
103-2-4
104-1
MDS_H
MDS_L
S
xE
xA
x5
x5

FIG. 30

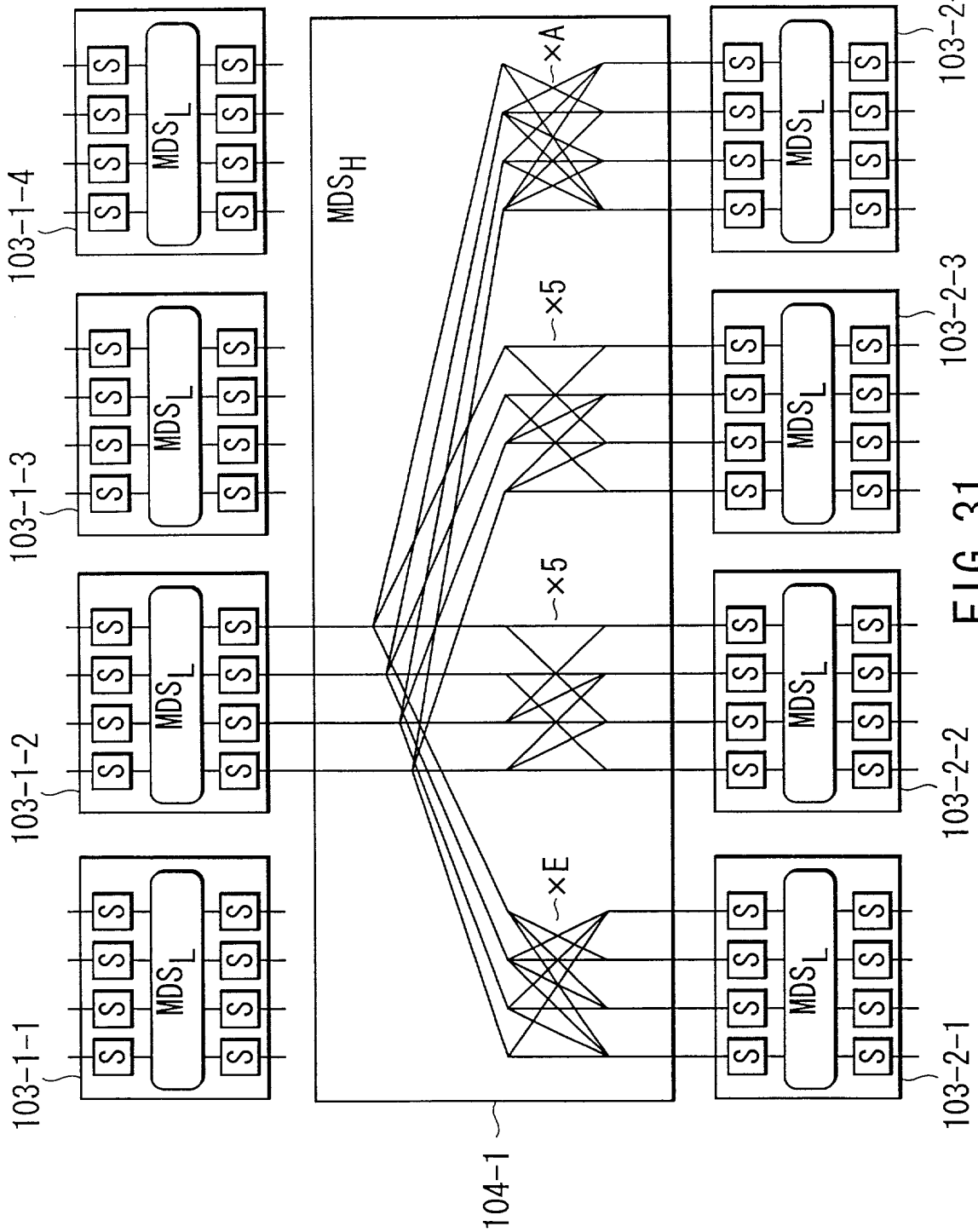

103-1-1
103-1-2
103-1-3
103-1-4
MDS_L
MDS_H
104-1
xE
x5
x5
xA
103-2-1
103-2-2
103-2-3
103-2-4
S

FIG. 31

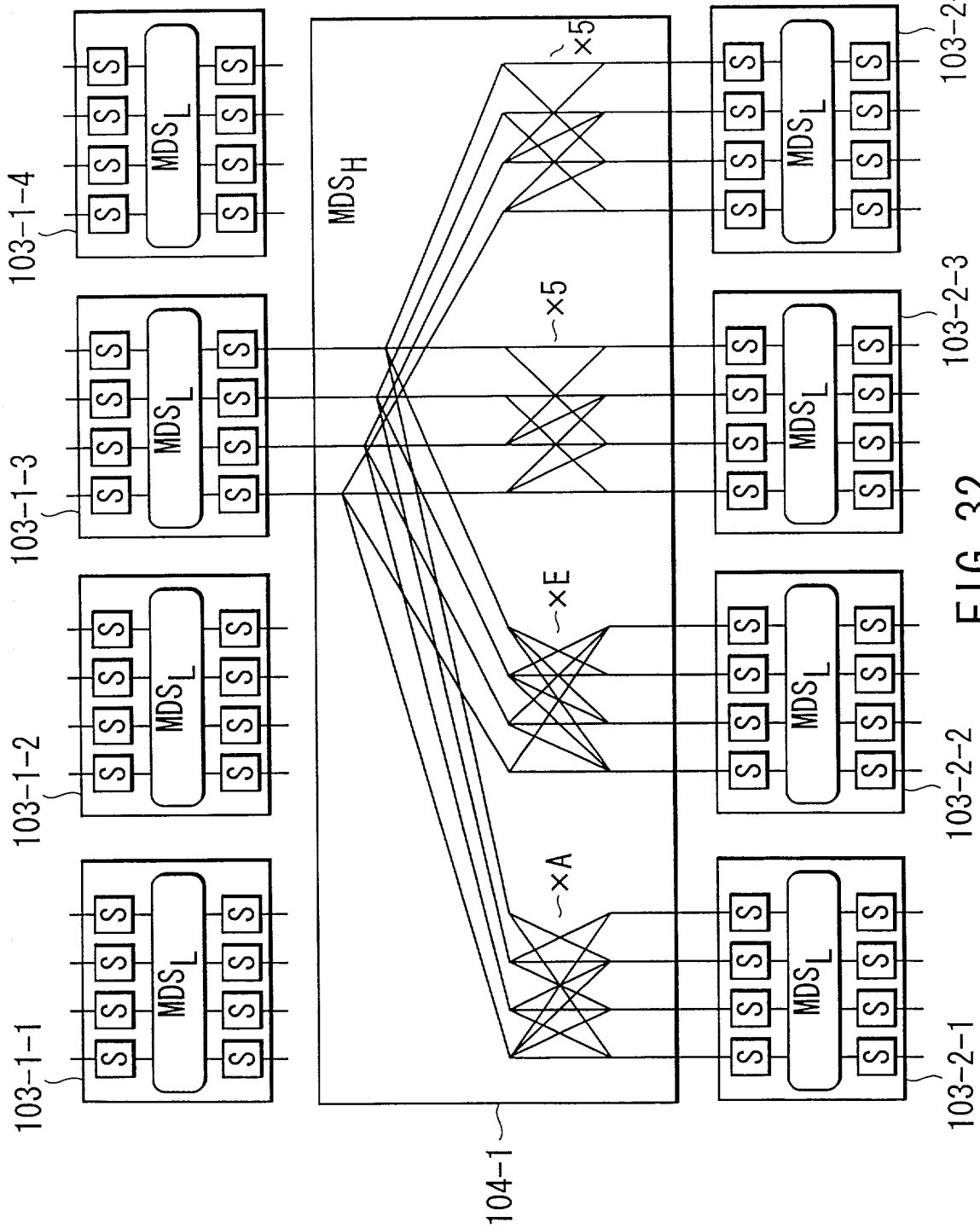

103-1-1
103-1-2
103-1-3
103-1-4
MDS_L
MDS_H
104-1
×A
×E
×5
×5
103-2-1
103-2-2
103-2-3
103-2-4
S

FIG. 32

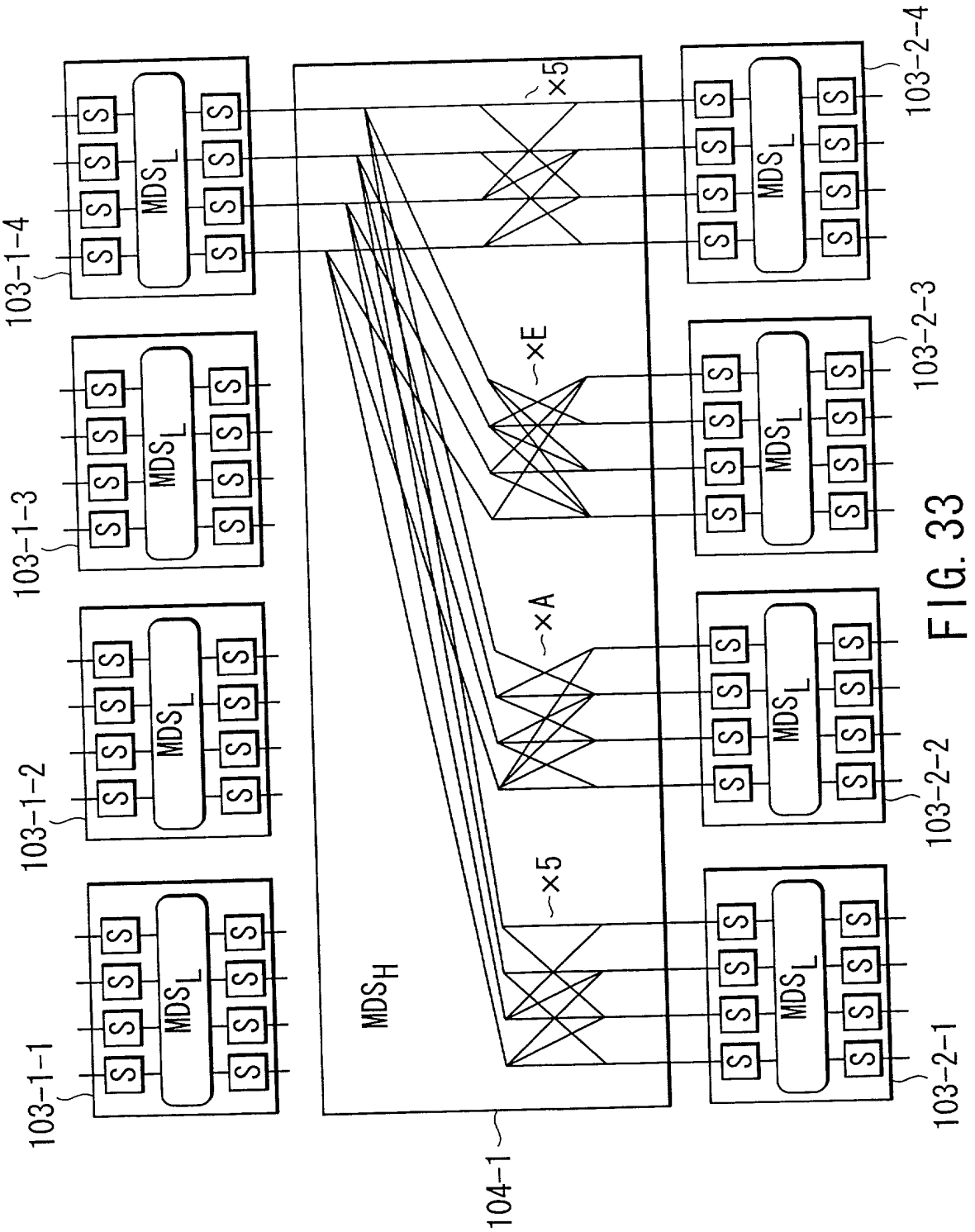

103-1-1
103-1-2
103-1-3
103-1-4
MDS_L
MDS_H
104-1
x5
xA
xE
x5
103-2-1
103-2-2
103-2-3
103-2-4

FIG. 33

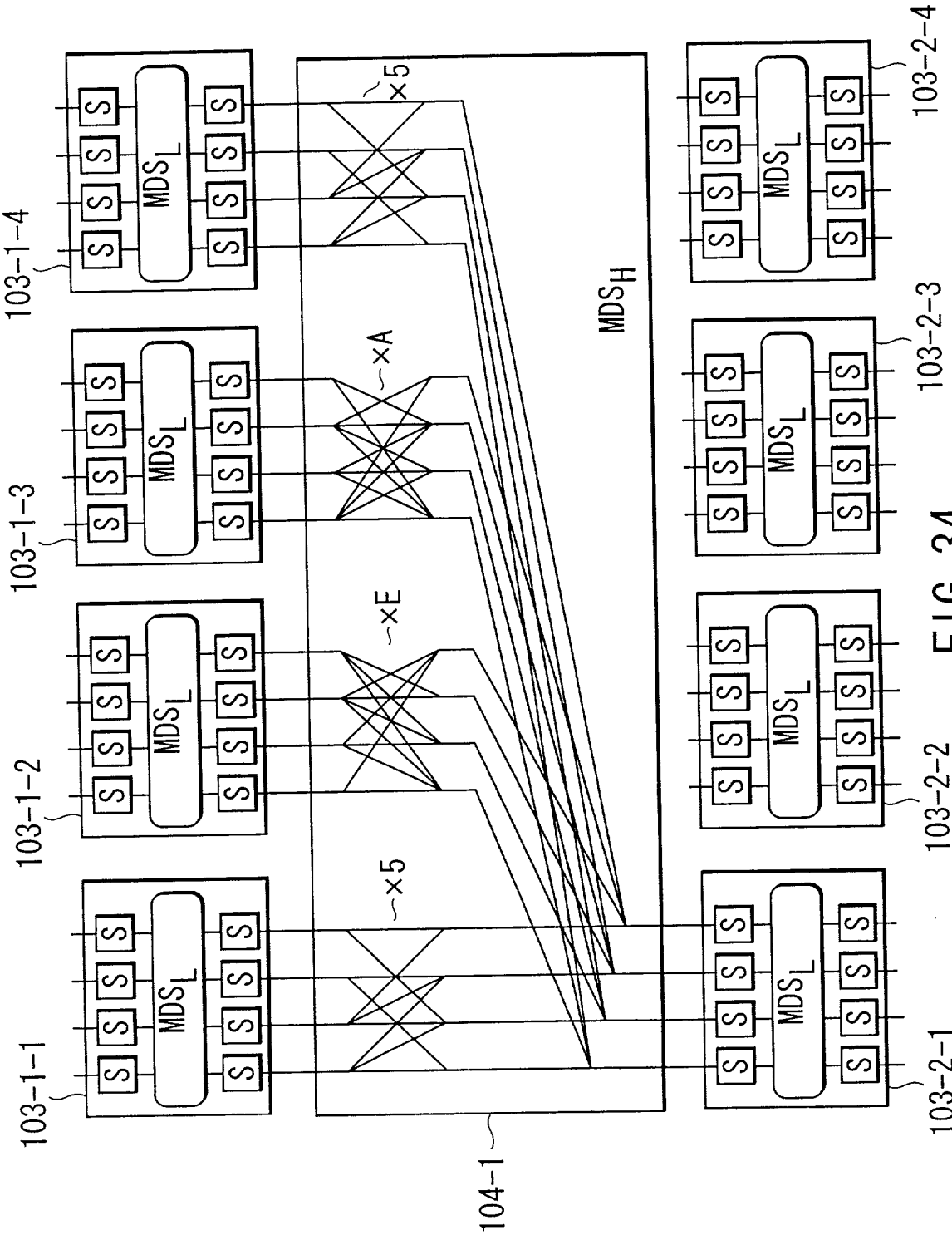

103-1-1
103-1-2
103-1-3
103-1-4
103-2-1
103-2-2
103-2-3
103-2-4
104-1
MDS_L
MDS_H
S
×5
×E
×A
×5

FIG. 34

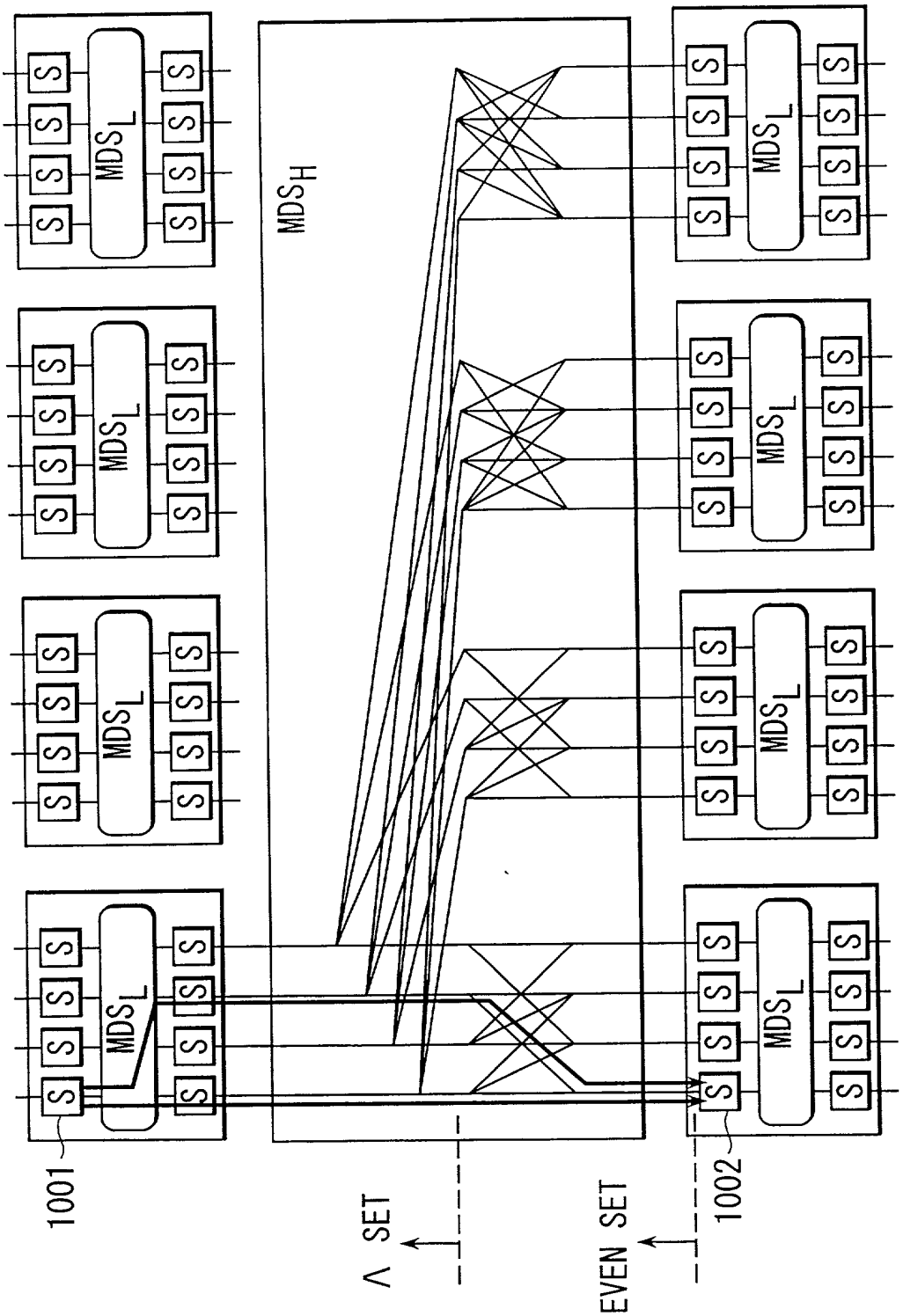


FIG. 35

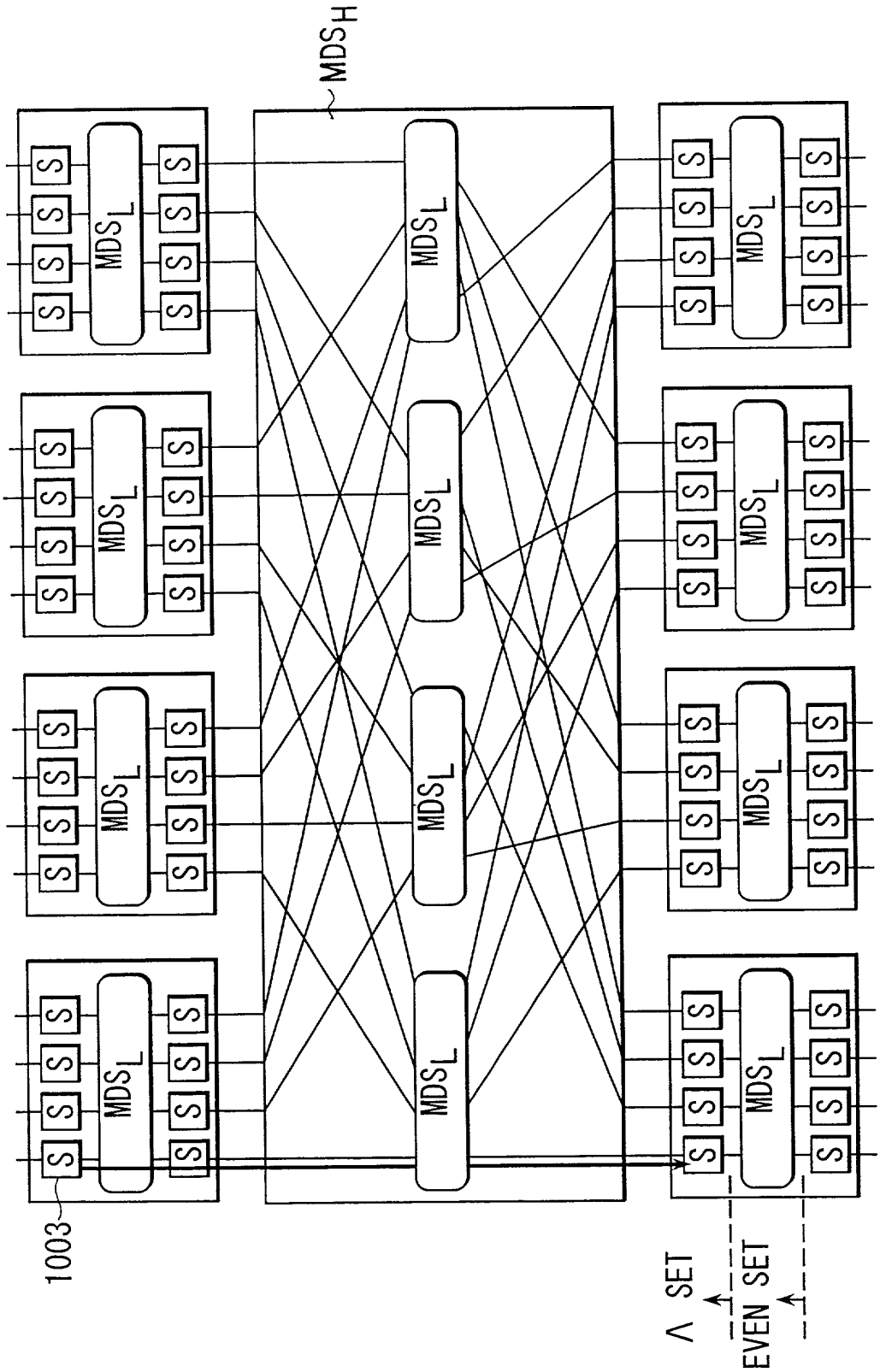


FIG. 36

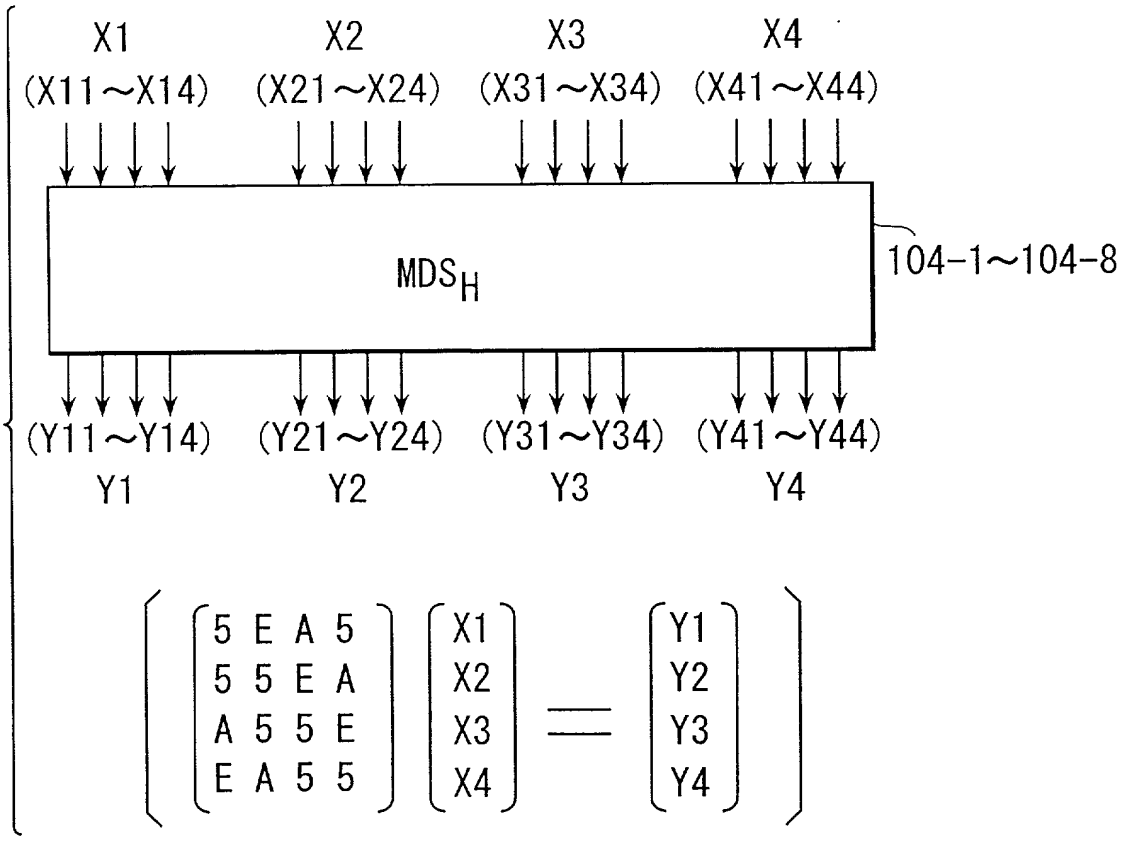

X1
(X11～X14)
X2
(X21～X24)
X3
(X31～X34)
X4
(X41～X44)
MDS$_H$
104-1～104-8
(Y11～Y14)
Y1
(Y21～Y24)
Y2
(Y31～Y34)
Y3
(Y41～Y44)
Y4
5 E A 5
5 5 E A
A 5 5 E
E A 5 5
X1
X2
X3
X4
Y1
Y2
Y3
Y4

FIG. 37

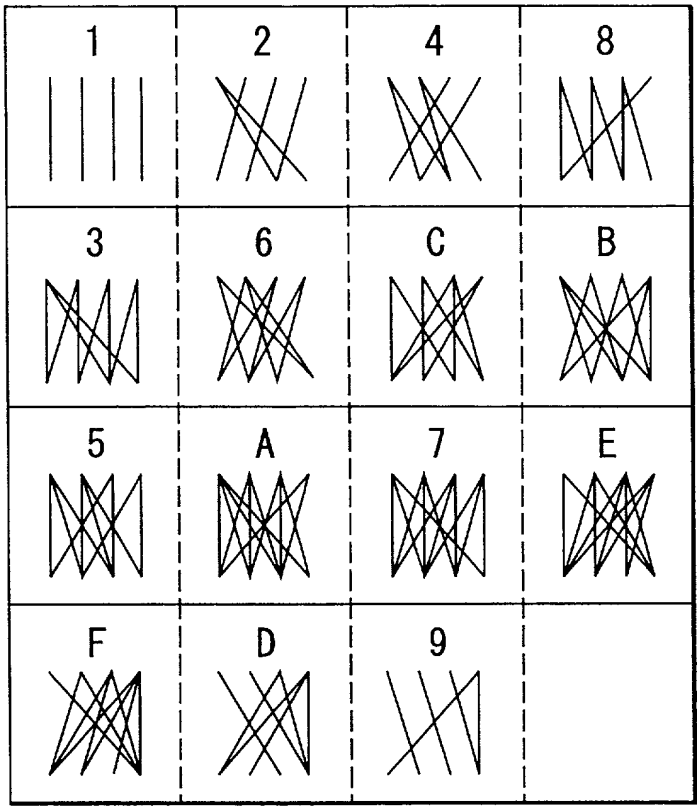


FIG. 38

FIG. 39A

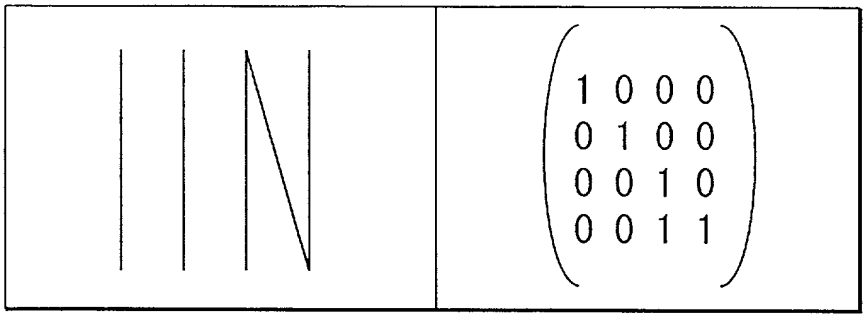


FIG. 39B

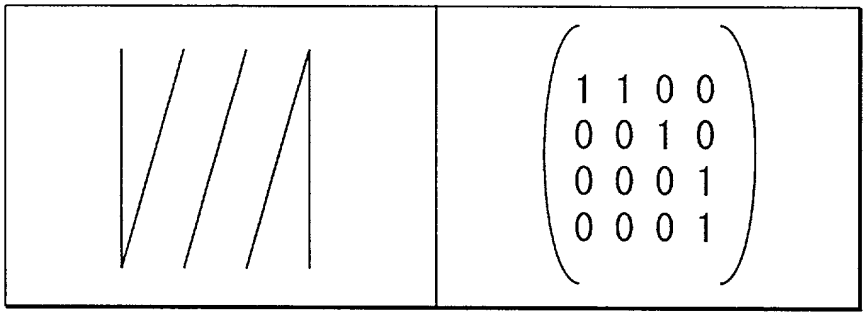


FIG. 39C

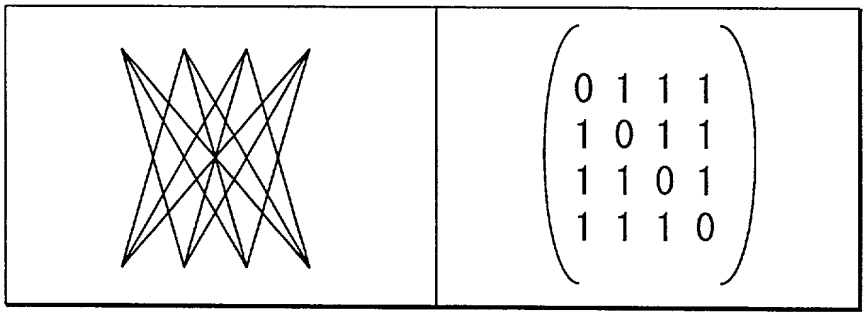
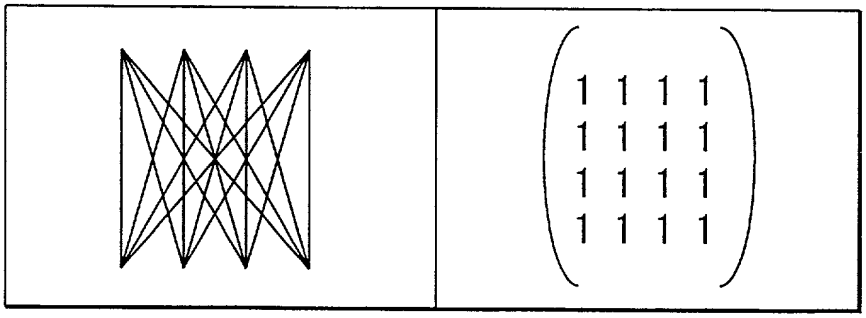


FIG. 39D



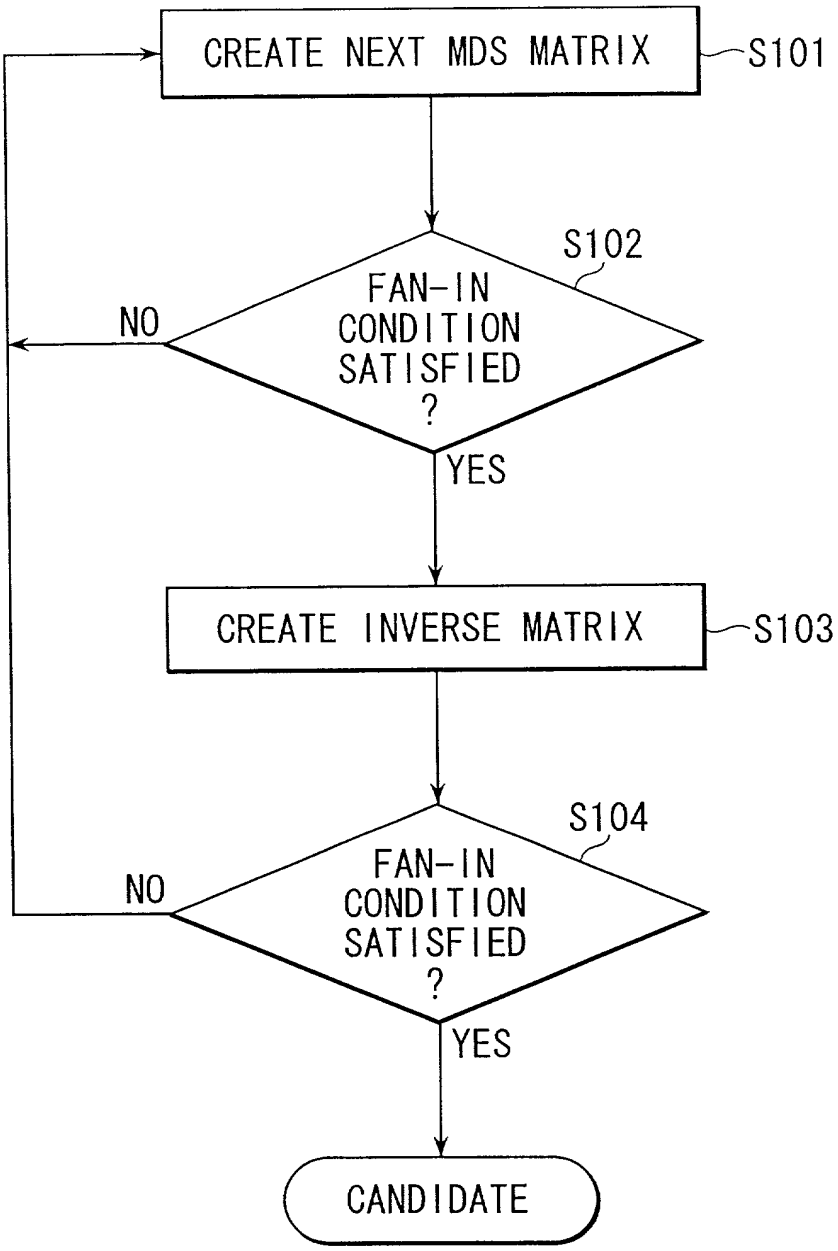

CREATE NEXT MDS MATRIX
S101
S102
FAN-IN CONDITION SATISFIED ?
NO
YES
CREATE INVERSE MATRIX
S103
S104
FAN-IN CONDITION SATISFIED ?
NO
YES
CANDIDATE

FIG. 40

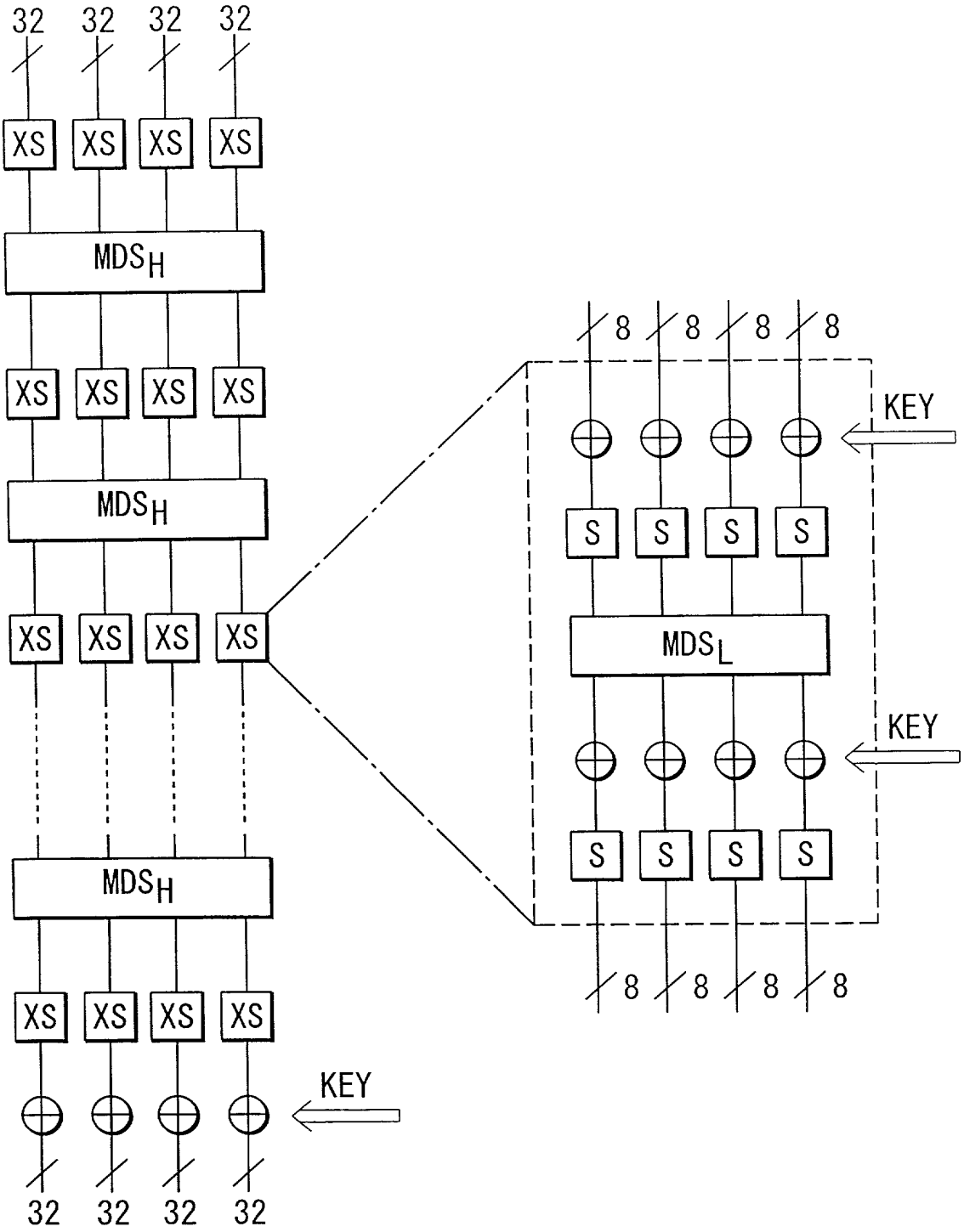


FIG. 41

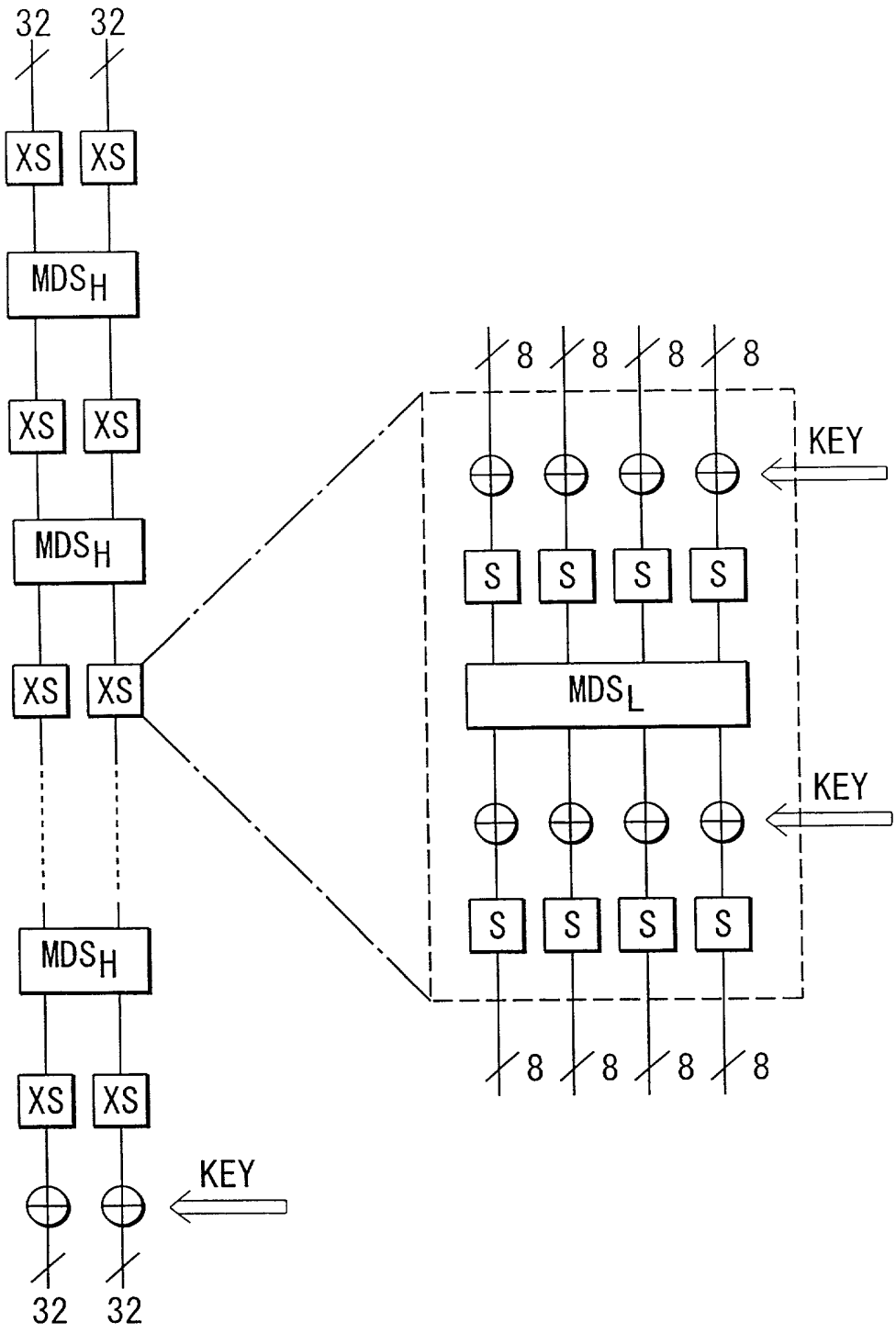

32
32
XS
XS
MDS$_H$
XS
XS
MDS$_H$
XS
XS
MDS$_H$
XS
XS
KEY
32
32
8
8
8
8
KEY
S
S
S
S
MDS$_L$
KEY
S
S
S
S
8
8
8
8

FIG. 42

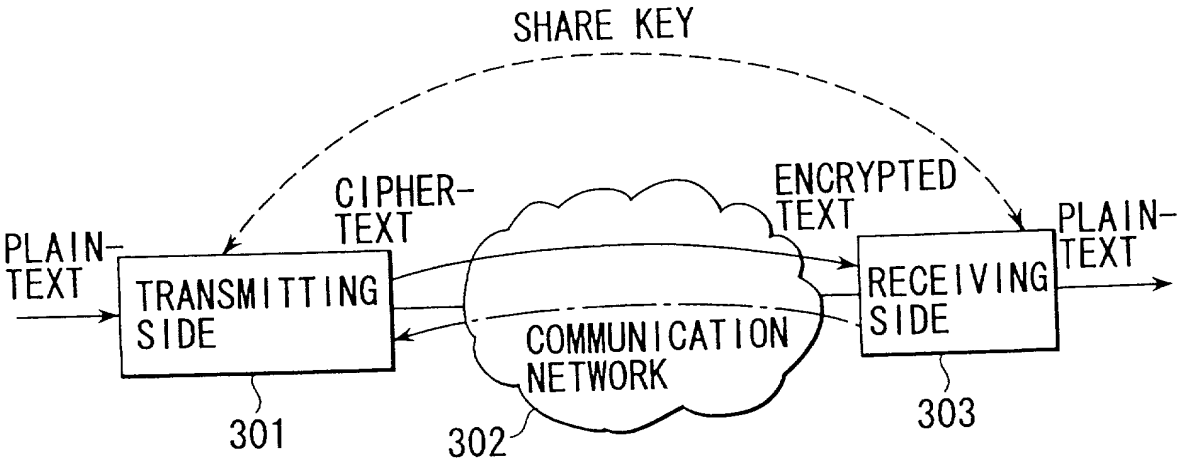


FIG. 43

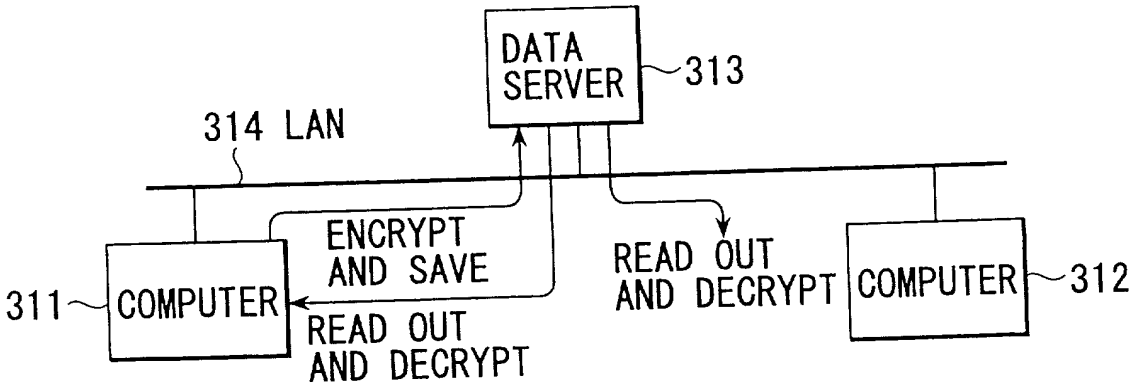


FIG. 44

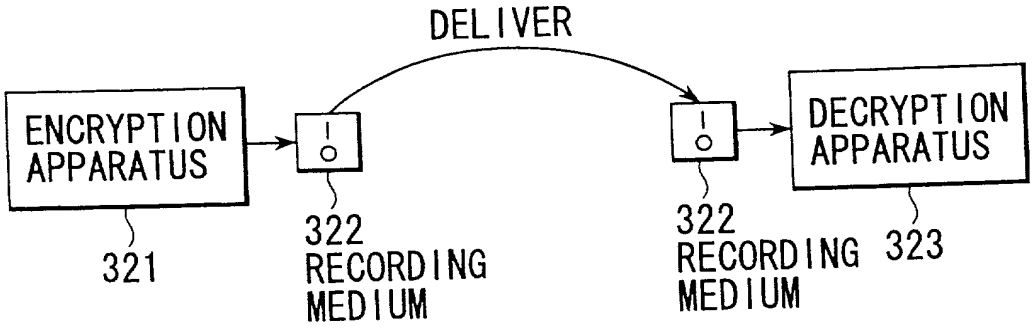


FIG. 45